UNIVERSITÀ DEGLI STUDI DI PADOVA


Dipartimento di Diritto Privato e Critica del Diritto
Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea Magistrale in
Giurisprudenza
Anno Accademico 2022/2023

# LA PRIVACY IN AZIENDA: GDPR E D. LGS. 231/2001, PUNTI DI CONTATTO E DIVERGENZE

Relatore: Chiar.mo Prof. Angelo Zambusi

Correlatrice: Chiar.ma Prof.ssa Alice Ferrato

Laureanda: Lucia Friso

Matricola: 1198165

**INDICE**

## ABSTRACT

La Rivoluzione informatica ha avuto un impatto notevole in ogni aspetto della nostra vita, ha portato alla diffusione di nuove forme di illeciti che devono essere efficacemente contrastati. Di questo cambiamento radicale ne risentono particolarmente le aziende, che si trovano a dover operare in una nuova realtà con problemi del tutto nuovi.

Il presente elaborato analizza brevemente il rapporto tra il diritto penale e le tecnologie informatiche, ripercorrendo le tappe che hanno portato alla creazione del *Cyberspace* e con esso a nuove forme di illeciti penali.

Al secondo capitolo si analizza nel dettaglio la struttura del *General Data Protection Regulation* (UE) 679/2016, anche detto GDPR, che nasce quale strumento essenziale per tutelare il Diritto alla *privacy*, ormai considerato alla stregua di diritto fondamentale per la protezione della propria sfera privata, di ciò che ne fa parte e delle informazioni personali.

Al terzo capitolo si affronta lo studio del D. Lgs. 231/2001, normativa che ha portato all'abbandono definitivo del dogma "*societas delinquere non potest*" e ha concretizzato la responsabilità amministrativa da reato dell'ente, spostando l'attenzione sul ruolo che le aziende rivestono nel caso in cui siano commessi reati informatici da soggetti facenti parte del loro organico.

Le aziende sono destinatarie dirette di entrambe le normative appena dette e devono obbligatoriamente adeguarsi in modo rigoroso a quanto in esse viene disposto, rischiando altrimenti di essere gravemente sanzionate.

Le imprese per ottemperare al GDPR e al D. Lgs. 231/2001 devono creare un'organizzazione interna con politiche e procedure ben precise, in particolare, ci si riferisce al Modello di Organizzazione, Gestione e Controllo (MOGC) e al Modello Organizzativo Privacy (MOP). Brevemente, il MOP è caratterizzato dall'insieme di misure tecniche ed organizzative adeguate alla protezione dei dati personali e in grado di soddisfare il principio di *accountability*. Il MOGC è un sistema che, se adottato ed attuato efficacemente, previene la realizzazione di illeciti all'interno dell'azienda e permette all'ente, nel caso detti illeciti siano commessi da soggetti che lo compongono, di

comprovare che la commissione del reato non sia eziologicamente collegabile ad una sua colpa organizzativa.

L'obbiettivo principe è comprendere se vi può essere un legame tra i sistemi organizzativi ed approfondirlo evidenziandone le differenze e le somiglianze; con l'auspicio di riuscire a trovare una soluzione, affinché le imprese siano sollevate da alcuni dei numerosi incombenti richiesti. La soluzione migliore, secondo diversi autori, si inserisce in un'ottica di integrazione, cercando di comprendere se le somiglianze siano tali da permettere un coordinamento tra le due normative, con una *compliance* unica, integrata e l'adozione di un Modello organizzativo comune in grado di prevenire, allo stesso tempo, le violazioni in materia di protezione dei dati personali e la commissione dei reati presupposto.

La ricerca di coordinamento dovrebbe essere l'aspirazione delle realtà aziendali, in modo che possano beneficiare di un risparmio di costi e di lavoro. Ma, è importante ricordare che in questa ricerca ci si dovrà calare in ciascuna realtà aziendale, per capire se il coordinamento è adatto all'impresa di riferimento, tenendo conto dell'attività svolta, dei rischi annessi e valutando se la struttura del Modello adottato per la prevenzione dei reati presupposto sia, eventualmente, compatibile anche per il rispetto delle disposizioni previste in ambito *privacy*.

Infine, si sottolinea che, nonostante i numerosi punti di contatto tra GDPR e D. Lgs. 231/2001, vi sono anche delle divergenze tali che potrebbero rendere impossibile l'auspicata integrazione.

# CAPITOLO I

# IL DIRITTO PENALE E LE TECNOLOGIE INFORMATICHE

SOMMARIO: 1.1. La rivoluzione cibernetica. – 1.2. La criminalità nel *Cyberspace*. – 1.2.1. I reati informatici. – 1.2.2. I reati cibernetici. – 1.3. Impatto sul diritto penale sostanziale: nuovi beni giuridici da tutelare, nuove condotte e nuovi fatti di reato. – 1.4. Evoluzione normativa, nell'ordinamento italiano e sovranazionale. – 1.5. La nascita del Diritto alla *privacy*.

## 1.1. *La rivoluzione cibernetica*

Nella realtà odierna, a fronte di uno sviluppo tecnologico tale che ha portato a definirla come "società dell'informazione", il diritto penale si trova ad affrontare nuove e affascinanti sfide. Per prima cosa vi è il generale ed inevitabile problema che deve affrontare il legislatore in qualsiasi campo del diritto ovvero quello di creare e modificare la normativa per poter essere al passo coi tempi e adattarla così sviluppo sociale, economico e tecnologico[1].

Le "tecnologie dell'informazione e della comunicazione" c.d. TIC[2] permettono di elaborare, comunicare, memorizzare e diffondere dati e informazioni di ogni genere, con una rapidità e semplicità prima sconosciute; la loro rapida evoluzione ha fatto si che possano applicarsi in ogni settore della vita sociale ed economica.

Queste nuove tecnologie permeano ogni aspetto della nostra vita quotidiana e, inevitabilmente, entrano in contatto con il diritto vigente nel nostro ordinamento.

[1] Per "società dell'informazione" si intende un contesto in cui le nuove tecnologie informatiche e di telecomunicazione assumono un ruolo fondamentale nello sviluppo delle attività umane (cit. G. SIRILLI, *Enciclopedia della Scienza e della Tecnica*, Voll. I-VI Lessico, Istituto dell'Enciclopedia Italiana, Roma, 2008, p. 422).

[2] In inglese ICT "*Information and Communications Technology*", intese come: un insieme di metodi e di tecniche utilizzate nella trasmissione, ricezione ed elaborazione di dati e informazioni.

Il diritto è una scienza sociale e in quanto tale non può restare indifferente agli effetti prodotti dall'impiego delle tecnologie informatiche all'interno della società; tali effetti sono spesso caratterizzati da nuovi rischi e nuovi problemi giuridici che implicano un necessario e costante adattamento del diritto.

Si è così creato un nuovo rapporto tra il diritto, in particolare, ciò che interessa questo elaborato, il diritto penale, e le nuove tecnologie informatiche. Da molti anni questo rapporto è oggetto di interesse della dottrina, della giurisprudenza, di diversi organismi internazionali e dei legislatori.

I legislatori intervengono con urgenza, per fronteggiare situazioni di incertezza, lacune normative e, in generale, per adattare il diritto a questo nuovo contesto sociale in continua evoluzione, spesso però non lo fanno con organicità, sistematicità e di pari passo con l'evoluzione tecnologica questo a causa del difficile inquadramento giuridico delle nuove fattispecie di reato informatico.

I cambiamenti si stanno imponendo con forza crescente, anche su settori più tradizionali della dottrina penale, la quale di frequente si trova a dover mettere in discussione principi ormai consolidati.

L'obbiettivo auspicato è di adattare il diritto ai nuovi cambiamenti e di raggiungere un'organicità tale da permettere una certezza del diritto; tale obbiettivo non appare di facile realizzazione, anche per il carattere fortemente transfrontaliero delle condotte criminali per le quali una disciplina omogenea appare imprescindibile, altrimenti vi sarebbe una situazione di incertezza, insicurezza e vulnerabilità.

Il diritto penale sostanziale e processuale ha fortemente risentito di queste innovazioni in ambito informatico e dev'essere necessariamente analizzato con un nuovo e diverso punto di vista. Non si può più parlare di un settore speciale del diritto penale e processuale penale, denominato "Diritto penale dell'informatica"[3], in quanto ad oggi si

[3] Il Diritto penale dell'informatica è il complesso di norme che riguarda i reati perpetrati attraverso le tecnologie dell'informazione. È pure, tuttavia, il risultato dell'interpretazione fornita dalla dottrina e dalla giurisprudenza. È anche, infine, il prodotto di una società che registra, quale rovescio della medaglia, il consolidarsi della criminalità informatica nelle sue diverse declinazioni, quale atto del singolo o di organizzazioni strutturate (cit. P. GALDIERI, *Il Diritto penale dell'informatica: legge, giudice e società*, G. Giappichelli Editore, Torino, abstract, 2021).

innesca una prospettiva molto più ampia, per cui è necessario riconsiderare l'intero ordinamento penale alla luce di questa rivoluzione.

La "rivoluzione informatica", o anche detta cibernetica[4], deriva da diversi sviluppi ed eventi che nel corso del tempo hanno contribuito ad un rapido avanzamento delle "tecnologie dell'informazione e della comunicazione" e della digitalizzazione della società.

Si può parlare di "rivoluzione" perché tale processo ha avuto un impatto significativo sulla società, sull'economia e sulla cultura, trasformando profondamente il modo in cui viviamo, lavoriamo e comunichiamo.

Gli effetti sociali sono ormai sotto gli occhi di tutti, soprattutto perché, queste novità che sembrava dovessero portarci verso un futuro migliore stanno viceversa ingabbiando sempre di più la nostra vita quotidiana. La digitalizzazione apre opportunità senza precedenti alla società, ma pone anche una serie di preoccupazioni, la consapevolezza di ciò sta pian piano crescendo[5].

Tale rivoluzione ha inevitabilmente determinato "nuovi conflitti" resi possibili da "nuovi comportamenti illeciti" che possono minacciare dei "nuovi diritti ed interessi" ritenuti meritevoli di tutela.

È nata una nuova "realtà digitale" nella quale si sviluppano rapporti personali ed interpersonali, in ambito pubblico e privato, economico e culturale, nazionale e sovranazionale, con il supporto di dispositivi mobili[6] sempre più efficienti, incidendo sull'organizzazione e sul funzionamento complessivo del sistema economico, sociale e politico.

---

[4] Il termine "cibernetica" fu coniato da Norbert Wiener nel 1947. Deriva dalla parola greca *kyber*, che significa "timoniere o pilota". La cibernetica studia i meccanismi di controllo e comunicazione con il mondo esterno degli organismi viventi e delle macchine. Questo campo di studio ha gettato le basi per la comprensione dei sistemi complessi e ha aperto la strada all'automazione e all'intelligenza artificiale.

[5] cit. E. NARDELLI, *La rivoluzione informatica: conoscenza, consapevolezza e potere nella società digitale*, Edizioni Themis, 2022, p. 245.

[6] Per dispositivo mobile si intende, in generale, qualsiasi dispositivo dotato di comunicazione *wireless* in grado di accedere alle funzioni di rete, come navigare sul *web*, consultare la posta elettronica e interagire con i *social network*, per es. un telefono cellulare, uno *smartphone* o un altro strumento (spesso multimediale), (cit. P. MAROCCO, Vocabolario Treccani online, in *treccani.it*, 2015).

Il concetto di "rete"[7] appare ormai riduttivo in quanto idoneo a delineare unicamente l'aspetto tecnico e materiale. Oggi si preferisce utilizzare il termine *Cyberspace*[8] che evoca l'idea di uno spazio virtuale, globale ed interattivo, nel quale siamo immersi e dove viene trasfuso ogni aspetto della nostra vita quotidiana. In questo nuovo spazio informatico globale, si assiste ad una dislocazione dei rapporti personali, economici, sociali e giuridici.

A partire dalla seconda metà degli anni '90 si è verificato un importante cambiamento: l'apertura di *Internet* ad un numero indistinto di utenti, creando una rete globale aperta, il c.d. *World Wide Web*[9]. Gli illeciti commessi all'interno di questa nuova rete globale si definiscono come *Cybercrime* e non più *Computercrime*.

Questo cambiamento segna l'inizio di una nuova fase, "l'epoca di *Internet*" nella quale si espandono i rapporti sociali ed economici, pubblici e privati, che si svolgono interamente in rete; la rete diventa un luogo virtuale nel quale si possono svolgere differenti attività, anche illecite ed offensive.

Il termine "*Computercrime*" venne utilizzato dal legislatore italiano del 1993, con la prima legge contro la criminalità informatica[10], per riferirsi ai reati realizzabili da sistemi operativi *stand alone*[11], connessi in reti telematiche chiuse o ad accesso circoscritto.

L'apertura di *Internet* al pubblico ha portato con sé diverse conseguenze, tra le quali: rendere sempre più frequenti i reati cibernetici, che possono essere realizzati da chiunque e sono in grado di colpire potenzialmente qualsiasi vittima sia connessa al *web*, sia estranea. Non è possibile delineare i singoli illeciti in maniera univoca attraverso un sistema chiuso; infatti, ad oggi si utilizza un sistema aperto, in continua evoluzione,

---

[7] Le reti informatiche collegano tra loro più *computer* o apparecchiature informatiche, in modo da condividere gli stessi dati e scambiarsi rapidamente documenti (cit. N. NOSENGO, Treccani online, in *treccani.it*, 2006).

[8] Termine coniato da William Gibson, scrittore canadese, nel suo romanzo *Neuromance* del 1984.

[9] Tim Berners Lee, nel 1989, inventò, insieme a Robert Cailliau, il *World Wide Web* ("www"), un sistema che permetteva la consultazione collettiva via *Internet* di pagine *web* raggiungibili tramite *link*.

[10] Ci si riferisce alla L. 21/12/1993, n. 547.

[11] Per sistema operativo *stand alone* si intende: dispositivo di *hardware* o *software* che non necessita di collegamenti esterni (cit. Dizionario di Italiano, in *hoepli.it*).

caratterizzato da una molteplicità indefinita di illeciti, di modalità di offesa e di diritti e interessi giuridici tutelati.

Il *web* è diventato interattivo, l'utente *online* può interagire con i contenuti e gli altri utenti, non si tratta più di una semplice consultazione passiva dei contenuti, ma di un coinvolgimento attivo nell'esplorazione, nella partecipazione e nell'interazione con il *web*. Questo rende ciascun fruitore del servizio *web*, allo stesso tempo, una potenziale vittima di illeciti oltre che un potenziale autore di reati lesivi di diritti e interessi altrui.

Negli ultimi tempi, grazie a questa apertura e coinvolgimento generalizzato, *Internet* è diventato parte integrante della vita di ciascuno di noi, non riusciamo e non possiamo farne a meno. Questo vale, in particolare, per i "nativi digitali"[12] che utilizzano questo nuovo spazio per comunicare senza limiti, senza barriere fisiche o psicologiche; difficilmente riescono a distinguere il mondo virtuale dal mondo reale e spesso sono soggetti vulnerabili poiché minori[13], tra i quali si sviluppano fenomeni allarmanti come il *revenge porn* e il *cyberbullismo*[14] con effetti preoccupanti sullo sviluppo personale e sull'inserimento nella vita reale.

In passato, il *web*, cosiddetto *web 1.0*, era caratterizzato da un flusso unidirezionale, l'utente agiva come destinatario passivo di informazioni e comunicazioni fornite dai

[12] Il termine "nativi digitali" è stato coniato dallo scrittore statunitense Marc Prensky e utilizzato per la prima volta nel suo articolo "*Digital Natives, Digital Immigrants"* del 2001; ci si riferisce a coloro che fin dalla nascita hanno vissuto a contatto con i mezzi di comunicazione digitali e le svariate tecnologie emerse negli ultimi anni, ad esempio i *social network*, *blog*, ma anche *tablet*, *smartphone* e *computer*.

[13] Si intende minori nell'accezione giuridica, secondo la quale: sono i soggetti che non hanno ancora compiuto il diciottesimo anno di età, tale condizione ha rilievo civile sulla relativa capacità di agire *ex* art. 2 c.c. e penale, sull'imputabilità *ex* art. 85 c.p.

[14] Secondo l'art. 1, comma 2 della Legge n. 71/2017,"Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del *cyberbullismo*" per *cyberbullismo* si intende: «*qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali realizzati, per via telematica, a danno di minori, nonché la diffusione di contenuti on line riguardanti uno o più componenti della famiglia di un minore con lo scopo di isolarlo, attaccarlo o metterlo in ridicolo*». Mentre, Il *revenge porn*, consiste nell'invio, consegna, cessione, pubblicazione o diffusione, da parte di chi li ha realizzati o sottratti e senza il consenso della persona cui si riferiscono, di immagini o video a contenuto sessualmente esplicito destinati a rimanere privati (Cit. Garante per la protezione dei dati personali, in *garanteprivacy.it*).

cosiddetti "*webmasters*"[15], una cerchia ristretta di soggetti; il *web* venne definito da Tim Berners Lee[16] un "*only read web*".

Seguendo l'evoluzione passo dopo passo, negli anni 2000 si sviluppa il *web 2.0* nel quale gli utenti possono interagire attraverso *blog*, *forum* e *social network*; nel 2006 si è cominciato a parlare di *web 3.0* con il quale si realizzano comunicazioni multimediali attraverso immagini, audio e video; infine, oggi si parla di *web 4.0* non ancora definito in maniera univoca, essendo in costante evoluzione, ma nel quale si può, tra le tante novità, ricondurre l'Intelligenza Artificiale[17].

Nel *Cyberspace*, gli utenti sono considerati come "risorse" da cui prelevare sistematicamente dati e informazioni di ogni tipo, qualsiasi azione ed operazione nel *web* viene elaborata da sofisticati algoritmi per sviluppare attività economiche, produttive e di ogni altro genere. La navigazione in *Internet* non è più autonoma, ma viene costantemente influenzata e guidata; ogni nostra scelta viene suggerita o memorizzata per poter influenzare le nostre scelte successive.

Questo costante controllo ha portato gli utenti a cercare degli espedienti in grado di eludere il sistema, tra i quali vi sono il "*dark web*" e "*deep web*"[18], si stanno sviluppando sempre di più permettendo la realizzazione di innumerevoli illeciti in grado di rimanere anonimi e privi di sanzione.

Il *novum* espresso dallo sviluppo della cibernetica è poter penetrare nell'agire umano, assumendone sia le capacità cognitive, intese come conoscenza e apprendimento

---

[15] Per "*webmaster*" si intende il responsabile dell'aggiornamento dei dati contenuti in un sito *internet*. Comprende un ampio ventaglio di competenze legate alla progettazione, realizzazione e gestione dei siti *web*, ed è la figura di riferimento per contatti e informazioni, soprattutto legate all'aspetto tecnico e di visualizzazione delle pagine da parte dei visitatori del sito (cit. Treccani online, Lessico del XXI Secolo, in *treccani.it*).

[16] Tim Barners Lee è un informatico britannico, co-inventore insieme a Robert Cailliau del *World Wide Web* e vincitore del premio Turin 2016.

[17] L'Intelligenza Artificiale (in inglese, *Artificial Intelligence* o AI) consente alle macchine di imparare dall'esperienza, di adeguarsi a nuove informazioni ricevute e svolgere compiti simili a quelli dell'uomo.

[18] Per "*dark web*" si intende la parte più "oscura" del *web*, costituita da "reti oscure", che si raggiungono attraverso specifici software, configurazioni e accessi autorizzativi, in cui si svolgono frequentemente attività illecite, per le tecniche di anonimizzazione che mascherano la provenienza; per "*deep web*" si intende quella parte del *web* non indicizzata dai motori di ricerca, perché non accessibile, né esplorabile dai comuni browser (cit. A. CADOPPI [et. al.], *Cybercrime*, I ed., UTET Giuridica, Milano, 2019, p. 39, nota 9).

dal mondo esterno, attraverso l'acquisizione di informazioni e dati da elaborare e memorizzare, sia le capacità di auto-determinarsi di conseguenza, per giungere a scelte operative che possono essere immediatamente attuate, fra possibili operazioni alternative[19].

Oggi si parla di equivalente della "volontà" umana espressa dai sistemi intelligenti, che viene riconosciuta a livello giuridico, con un rilievo anche nel diritto penale, come nel caso della validità di negozi giuridici conclusi automaticamente, che le persone a cui si imputano non avrebbero altrimenti potuto porre in essere negli stessi tempi, contenuti e modi.

I sistemi cibernetici non sono più meri strumenti di cui possiamo disporre, ma sono diventati agenti autonomi che sollevano nuovi problemi d'imputazione di responsabilità, non solo penale, nelle ipotesi in cui arrecano danni ingiusti o comunque ledono beni giuridici individuali o collettivi, se non anche diritti fondamentali, come, per esempio, la libertà di opinione o di autodeterminazione. Anche la nostra *privacy*[20] ne risente, viene sacrificata, non riusciamo più ad escludere terzi dall'accesso alle nostre informazioni personali e a controllarne il trattamento, poiché prevale l'esigenza di una massima efficienza possibile dei sistemi automatizzati.

Ad oggi appare da subito evidente che questa Rivoluzione cibernetica ha reso necessaria l'elaborazione di un quadro sistematico generale, in cui collocare nuove regole di imputazione della responsabilità, che tengano conto delle peculiarità dei comportamenti e dei fatti penalmente rilevanti commessi o manifestati nel *Cyberspace*. In passato non si era di questa idea, per molto tempo venne mantenuto un approccio conservatore, per cui non era necessario riformare il diritto poiché si riconosceva alla

[19] Esemplificando: una *self driving car*, è tanto più affidabile quante più informazioni riesce autonomamente e velocemente a raccogliere dall'ambiente esterno, con sensori ottici, acustici, ecc. ed attraverso connessioni a terminali e sistemi di informazione presenti sulla rete stradale (cd. *smart road*) (cit. PICOTTI L. [et. al.]*, Il diritto penale dell'informatica all'epoca di internet,* CEDAM, Padova, 2004, p. 711, nota 6).

[20] Il termine inglese *privacy*, che significa "riservatezza", è diventato di uso comune per indicare la sfera privata di ogni individuo e quell'insieme di informazioni personali sulle quali desideriamo di mantenere il riserbo, escludendone l'accesso ad altri.

tecnologia una funzione autoregolatrice, ovverosia era la prassi, che nasceva tra gli operatori, a risolvere da sé diverse questioni, in tal modo, sostituendosi al diritto.

In poco tempo ci si rese conto dell'inadeguatezza di tale approccio, è utopistico ritenere che il *Cyberspace* sia uno spazio libero dal diritto; lo ha dimostrato il riconoscimento a livello mondiale della necessità di un "*Web Bill of Rights*"[21].

Partendo dal presupposto per ciò che è illecito *offline* non può essere lecito *online*, anche se si presenta con nuove e imprevedibili modalità e forme; il diritto dev'essere riplasmato sulla base di queste nuove forme di criminalità che toccano diritti e interessi da sempre tutelati ovvero nuovi diritti ed interessi che si creano in questo nuovo "mondo". Rimangono dubbi su come debba essere realizzato questo adeguamento, c'è chi ritiene che si sia creata un'autonoma branca del diritto, il "Diritto dell'informatica"[22], caratterizzata da norme specifiche, nuove e autonome rispetto alle norme tradizionali e chi, al contrario, nega questa autonomia e applica gli istituti tradizionali.

Nonostante la peculiarità dei beni informatici, la ridefinizione degli istituti tradizionali e la consapevolezza dei nuovi problemi, non si raggiunge un'unificazione dei fatti che, a causa degli obbiettivi perseguiti e dei contesti in cui si realizzano, finiscono inevitabilmente e spesso erroneamente, per essere integrati all'interno delle partizioni del sistema giuridico già esistente.

### 1.2. *La criminalità nel* Cyberspace

La criminalità nel *Cyberspace*, un problema crescente a livello globale, è caratterizzata da una vasta gamma di attività illegali che coinvolgono *computer*, reti, dispositivi digitali e l'ambiente *online*, è in continua evoluzione e presenta sfide uniche nell'applicazione della legge e nella sicurezza informatica.

[21] A livello nazionale una Commissione di studio presieduta da Stefano Rodotà, istituita dalla Presidenza della Camera dei Deputati del Parlamento italiano, ha presentato il 28 luglio 2015 una "Dichiarazione dei diritti di *internet*".

[22] Per "Diritto dell'informatica" ci si riferisce al complesso di norme che disciplinano l'uso delle tecnologie informatiche (cit. P. GALDIERI, *Il diritto penale dell'informatica: legge, giudice e società*, Giappichelli Editore, Torino, 2021, p. 2).

La criminalità informatica non è in una categoria definita giuridicamente, anche se compare in fonti europee e sovranazionali, poiché risulta essere flessibile ed aperta a fatti criminosi che possono essere commessi attraverso la rete o nel *Cyberspace*.

Questi crimini sfruttano le tecnologie digitali per commettere frodi, rubare informazioni sensibili, danneggiare sistemi informatici, violare la *privacy* e molto altro ancora.

Sul piano del diritto penale sostanziale si può ravvisare una classificazione sistematica dei reati informatici. Per prima cosa, si possono distinguere i "reati informatici" dai "reati cibernetici", nella prima categoria rientrano i reati che, per l'integrazione della fattispecie incriminatrice, richiedono un elemento informatico; mentre, nella seconda categoria rientrano i reati tradizionali ovvero i nuovi reati commessi all'interno dell'ambiente del *Cyberspace*.

### 1.2.1. *I reati informatici*

I reati informatici si suddividono in reati informatici in senso stretto e in senso ampio. Per "reati informatici in senso stretto" si intendono tutti i reati che sulla base della fattispecie incriminatrice fissata dalla norma hanno almeno un elemento, essenziale od occasionale, che richiama espressamente ed univocamente le TIC[23]; si tratta di un elemento che dev'essere integrato ai fini della consumazione del fatto di reato. Un esempio può essere l'accesso abusivo di cui all'art. 615-*ter* c.p.[24]: «*chiunque*

[23] Per TIC ci si riferisce sempre alle "tecnologie dell'informazione e della comunicazione".

[24] *Ex* art. 615-*ter* c.p.: «*1. Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. 2. La pena è della reclusione da uno a cinque anni: 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema; 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; 3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. 3. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla*

*abusivamente si introduce in un sistema informatico o telematico*», perciò ai fini della commissione del reato è necessario che l'accesso abusivo riguardi un sistema informatico o telematico[25].

Nella categoria "reati informatici in senso ampio" si inseriscono tutti i reati che possono realizzarsi anche mediate strumenti informatici o su dispositivi informatici, ovvero con modalità di condotta o effetti che coinvolgono le TIC. Gli elementi distintivi compaiono nella fattispecie legale come elementi eventuali ed alternativi ad altri che prescindono dalle TIC, ovvero, in certi casi, possono essere non esplicitamente previsti nella norma, ma da essa ricavabili in via interpretativa o comunque compatibili con essa.

Rientrano in questa categoria i reati in materia di tutela dei dati personali ai sensi degli artt. 167 e ss. del Codice della *Privacy*[26], i dati personali possono essere trattati sia in forma digitale che in forma cartacea.

Lo sviluppo delle TIC e la crescente diffusione del *Cyberspace* portano inevitabilmente ad ampliare sempre di più l'ambito di quest'ultima categoria. Un numero sempre crescente di reati viene commesso o potrebbe essere commesso *online* o utilizzando strumenti o oggetti informatici, anche se il legislatore non necessariamente lega l'esistenza del reato a tale eventualità, quest'ultima deve essere valutata caso per caso, sulla base delle circostanze concrete.

### 1.2.2. *I reati cibernetici*

I reati cibernetici sono tutti quelli che si commettono o si possono commettere nel *Cyberspace*. Con l'espandersi del *Cyberspace* questa categoria ha assunto un'importanza ed estensione via via maggiori, detti reati possono essere realizzati con

*sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. 4. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio*».

[25] Per "sistema informatico o telematico" si intende una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione di tecnologie informatiche (cit. Dizionario giuridico, in *brocardi.it*).

[26] Ci si riferisce al D. Lgs. n. 196/2003.

un'estrema facilità ed hanno un effetto lesivo maggiore di quello che si avrebbe in caso di commissione di tali reati con i tradizionali mezzi di comunicazione (quali la stampa, la radio, la televisione ecc.). Presentano un particolare rilievo giuridico e processuale, data la necessità di contrastarli con adeguate sanzioni penali, specifici strumenti di indagine e di raccolta e circolazione di prove.

Si tratta di una categoria aperta perché abbraccia una crescente molteplicità di illeciti, modalità di offesa di interessi giuridici e diritti che a loro volta possono configurarsi come nuovi.

Si possono a loro volta suddividere in reati cibernetici "in senso stretto" rispetto ai quali la fattispecie incriminatrice contiene un elemento specifico, necessario o circostanziale, che espressamente richiama la "rete"; e reati cibernetici "in senso ampio" nei quali la previsione legislativa richiede elementi di tipizzazione del fatto che implicitamente o in via interpretativa sono compatibili con la realizzazione nel *Cyberspace*; perciò, la commissione "in rete" si atteggia quale requisito eventuale ricavabile in via ermeneutica.

Nei primi l'elemento tecnologico e specializzante è caratterizzato proprio dalla connessione in rete o dalla fruibilità del *Cyberspace*. I secondi, invece, presentano la possibilità di realizzazione concreta "in rete" e sono formulati in termini più generali ed elastici, tanto da essere realizzabili o concepibili a prescindere dall'informatica e dalla rete[27].

I reati cibernetici in senso stretto coincidono con i reati informatici in senso stretto, poiché entrambi richiedono come elemento costitutivo della fattispecie incriminatrice la commissione nel *Cyberspace*, implicando logicamente un riferimento alle TIC. Tuttavia, non sempre è vero il contrario, poiché non tutti i reati informatici in senso stretto sono anche reati cibernetici in senso stretto; questo perché l'elemento che richiama le TIC non necessariamente richiede anche la commissione "in rete".

Un esempio emblematico di reato cibernetico in senso stretto è il c.d.

[27] cit. L. PICOTTI, *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in *riv. Trim. dir. Pen. ec*., 2011.

*cyberstalking* previsto all'art. 612-*bis*, comma 2, c.p., inserito dal D. L. n. 93/2013, convertito dalla L. n. 119/2013[28], come aggravante del reato di atti persecutori, il quale stabilisce: «*se il fatto è commesso attraverso strumenti informatici o telematici*»; si nota come la modalità che tipizza normativamente l'aggravante, con un elemento che richiama espressamente le TIC, si riferisce a condotte che possono realizzarsi nel *Cyberspace* pur producendo eventi consumativi nel mondo reale, come «*cagionare un perdurante e grave stato di ansia e paura*»[29].

Un esempio paradigmatico di reato cibernetico in senso ampio può essere la diffamazione *online* ai sensi dell'art. 595 c.p.[30], nel quale la condotta richiesta: «*comunicando con più persone*», pur non menzionando espressamente le TIC, è sicuramente compatibile le modalità di comunicazione nel *Cyberspace*.

Nell'analizzare questa suddivisione metodica è importante ricordare quanto disciplinato all'art. 14, par. 2, lett. c) [31] della Convenzione *Cybercrime* del 2001 per cui ogni reato può aver bisogno dell'acquisizione di prove elettroniche, questo non qualifica

---

[28] *Ex* art. 612-*bis*, comma 2 c.p.: «*La pena è aumentata se il fatto è commesso dal coniuge, anche separato o divorziato, o da persona che è o è stata legata da relazione affettiva alla persona offesa ovvero se il fatto è commesso attraverso strumenti informatici o telematici*»

[29] *Ex* art. 612-*bis*, comma 1 c.p.

[30] *Ex* art. 595 c.p.: «*1. Chiunque, fuori dei casi indicati nell'articolo precedente, comunicando con più persone, offende l'altrui reputazione, è punito con la reclusione fino a un anno o con la multa fino a milletrentadue euro. 2. Se l'offesa consiste nell'attribuzione di un fatto determinato la pena è della reclusione fino a due anni, ovvero della multa fino a duemilasessantacinque euro. 3. Se l'offesa è recata col mezzo della stampa o con qualsiasi altro mezzo di pubblicità, ovvero in atto pubblico, la pena è della reclusione da sei mesi a tre anni o della multa non inferiore a cinquecentosedici euro. 4. Se l'offesa è recata a un Corpo politico, amministrativo o giudiziario, o ad una sua rappresentanza, o ad una Autorità costituita in collegio, le pene sono aumentate*».

[31] *Ex* art. 14, par. 2, lett. c) della Convenzione del cybercrime: «*1. Le Parti adottano le misure legislative e di altra natura necessarie per definire le facoltà e le procedure previste nella presente sezione ai fini di indagini o procedimenti penali specifici. 2. Salvo disposizione contraria all'articolo 21, le Parti applicano le facoltà e le procedure menzionati nel paragrafo 1: a) ai reati previsti dagli articoli 2–11; b) a tutti gli altri reati commessi attraverso un sistema informatico; e c) all'acquisizione delle prove elettroniche di un reato. 3. a) Le Parti possono riservarsi il diritto di applicare le misure di cui all'articolo 20 solamente ai reati o alle categorie di reati specificati nella riserva, purché l'elenco di tali reati o categorie di reati non sia più circoscritto di quello dei reati ai quali le Parti applicano le misure di cui all'articolo 21. Le Parti verificano la possibilità di limitare tale riserva in modo da consentire un'applicazione quanto più ampia possibile della misura di cui all'articolo 20. b) Le Parti che, a causa dei limiti previsti dalla loro legislazione in vigore al momento dell'adozione della presente Convenzione, non siano in grado di applicare le misure previste agli articoli 20 e 21 alle comunicazioni trasmesse all'interno di un sistema informatico di un fornitore di servizi, che: i) è operativo per un gruppo definito di utenti, e ii) non utilizza reti pubbliche di telecomunicazione e non è collegato a un altro sistema informatico pubblico o privato, si possono riservare il diritto di non applicare dette misure a tali comunicazioni. Le Parti verificano la*

automaticamente il reato come cibernetico; in questi casi il fatto costitutivo di reato non si colloca neppure in parte nel *Cyberspace*, ma si verificano conseguenze sul piano del diritto penale processuale, poiché si richiede nell'accertamento probatorio la ricerca, verifica, acquisizione, conservazione e valutazione di elementi informatici e cibernetici.

### 1.3. *Impatto sul diritto penale sostanziale: nuovi beni giuridici da tutelare, nuove condotte e nuovi fatti di reato*

L'incidenza delle TIC e la nuova dimensione del *Cyberspace* innovano la configurazione delle condotte tipiche, i fatti costitutivi di reato integranti l'offesa di beni giuridici anch'essi corrispondentemente rinnovati rispetto a quelli tradizionali poiché coinvolgenti l'uso o l'applicazione della tecnologia informatica e digitale.

Fondamentale è lo strumento concettuale del bene giuridico che permette, in un quadro giuridico settoriale, frammentario e scarsamente coordinato, di dare un certo ordine attraverso una classificazione ordinata dei reati. Nel nostro codice penale il legislatore ha collocato sistematicamente alcuni dei principali reati informatici sulla base dei beni giuridici oggetto di protezione, conservando una corrispondenza e vicinanza rispetto alle fattispecie comuni preesistenti, le quali tutelano beni giuridici considerati "simili"; ma, in realtà, detta corrispondenza, tra beni giuridici nuovi e beni giuridici preesistenti, non è sempre effettiva, anzi, in alcuni casi, confrontandoli non si fa altro che evidenziare le specificità, novità e differenze dei nuovi beni giuridici.

I nuovi beni giuridici possono risultare identici, come nel caso del patrimonio, ovvero caratterizzati da analogie o comunque di rango non inferiore rispetto a quelli già protetti rispetto ad offese analoghe commesse *offline*.

Sono inevitabilmente emersi nuovi interessi meritevoli di una specifica e

*possibilità di limitare tale riserva in modo da consentire un'applicazione quanto più ampia possibile delle misure di cui agli articoli 20 e 21*».

autonoma tutela giuridica, anche di natura penale; in tal caso si può parlare di beni giuridici "nuovi" rispetto a quelli preesistenti.

Questi nuovi connotati dei beni giuridici che possono essere offesi nel *Cyberspace* conferiscono loro un'importanza fondamentale, come nel caso della "riservatezza informatica" e della "sicurezza informatica". La "riservatezza informatica" assurge a diritto fondamentale della persona, inteso quale spazio informatico esclusivo essenziale per la vita individuale e sociale che dev'essere lasciato libero da intrusioni di terzi; ormai distinta e autonoma rispetto al parimenti fondamentale diritto della tutela dei propri "dati personali", essendo superata la concezione riduttiva della *privacy* quale "*the right to be let alone*"[32]. Strettamente collegata appare la "sicurezza informatica", o c.d. *Cybersecurity*[33], che diventa oggetto di obblighi la cui violazione viene sanzionata penalmente. Oggi, grazie al Regolamento (UE) 2016/679, c.d. GDPR[34], vengono previsti obblighi di valutazione e prevenzione dei rischi, nonché di risposta adeguata a conseguenze avverse, sia in capo ai titolari dei trattamenti dei dati, ma anche ai responsabili della *privacy*, ai programmatori ecc. fin dalla fase della progettazione e configurazione dei sistemi[35]. La *Cybersicurity* arriva financo a configurarsi quale bene indisponibile collettivo, la cui gestione viene attribuita alle autorità governative, dotate di speciali poteri al riguardo.

Cambiano radicalmente anche le modalità di offesa, caratterizzate soprattutto da una maggiore diffusività, in quanto implicano l'utilizzo dei mezzi tecnologici; dunque, la *res informatica* non si considera solo come oggetto di tutela, ma anche come *instrumentum delicti*[36]. Lo dimostra il reato di frode informatica, collocato fra i delitti

---

[32] cfr. S.D. WARREN, L.D. BRANDEIS, *The Right to Privacy*, in *Harvard L. Rev.*, 1890.

[33] La *cybersecurity* è un insieme di processi, procedure consigliate e soluzioni tecnologiche in grado di proteggere la tua rete e i tuoi sistemi critici dagli attacchi digitali.

[34] Il "*General Data Protection Regulation*" è un regolamento europeo in materia di protezione dei dati personali.

[35] Ci si riferisce al concetto di "*privacy by design*" che ha lo scopo di garantire l'esistenza di un corretto livello di *privacy* e protezione dei dati personali fin dalla fase di progettazione (*design*) di qualunque sistema, servizio, prodotto o processo così come durante il loro ciclo di vita; quale si affianca il concetto "*privacy by default*" per il quale si esige che il titolare individui, prima di iniziare il trattamento dei dati, quali dati personali sono strettamente necessari, per la finalità specifica per cui sono stati acquisiti, ai fini di proteggere la riservatezza dei dati personali.

[36] cit. M. FUMO, *La condotta nei reati informatici,* in *Archivio Penale*, fascicolo 3, 2013.

contro il patrimonio, appare ispirato alla truffa comune avendo lo stesso disvalore penale, in termini di limiti edittali di pena, e gli stessi eventi consumativi. L'azione del reo non è però indirizzata ad un soggetto passivo persona fisica da indurre in errore, ma direttamente al sistema informatico di cui il reo altera il funzionamento per un interesse personale ovvero mediante qualsiasi altro intervento "senza diritto"[37] su dati, informazioni, programmi o qualunque file registrato nei sistemi informatici o telematici ovvero in supporti ad essi pertinenti, destinati ad essere utilizzati in un sistema informatico. Si nota come il legislatore utilizzi delle clausole aperte per definire le modalità di condotta, che per integrare la fattispecie di reato devono determinare la produzione degli eventi consumativi previsti.

Mutano gli oggetti passivi o materiali sui quali ricade la condotta criminosa, sono prodotti della tecnologia informatica e telematica che determinano una speciale configurazione del bene protetto. Un esempio emblematico è dato dal reato di falsità informatica, ai sensi dell'art. 491-*bis* c.p.[38] per il quale si applica la fattispecie di "falsità in atti" prevista all'art. 483 c.p.[39], quando l'oggetto è rappresentato da documenti informatici sia pubblici che privati. Il nuovo oggetto materiale è rappresentato dal "documento informatico", che rappresenta una nozione autonoma e distinta da quella del documento tradizionalmente inteso[40], la sua nozione anche se non espressamente chiarita, la si ricava in via interpretativa e nell'elaborazione dogmatica dalla disciplina civile ed amministrativa. Il documento informatico viene definito all'art. 1, lett. p) del D. Lgs.

[37] Per intervento "senza diritto" si intende un intervento abusivo, non autorizzato; su questo possono immaginarsi diverse ricostruzioni interpretative, per un approfondimento vd. A. CADOPPI, [et. al.], op. cit., pp. 833 ss.

[38] *Ex* art. 491-*bis* c.p.: «*Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici*».

[39] *Ex* art. 483 c.p.: «*1. Chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni. 2. Se si tratta di false attestazioni in atti dello stato civile [449], la reclusione non può essere inferiore a tre mesi*».

[40] Per "documento tradizionalmente inteso" ci si riferisce allo strumento che consente la formulazione di un giudizio circa l'esistenza di un fatto o atto, nonché la possibilità di sussumere il fatto o atto sotto una fattispecie normativa (cit. P. MILITE, *Documento e documentazione*, in *Riv. Giuridica Italiana*, 2000).

7/3/2005 e succ. mod., c.d. Codice dell'amministrazione digitale, come: «*rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*».

Questi nuovi elementi tecnologici incidono anche su altri aspetti, quali il nesso di causalità, che rappresenta il nesso di imputazione di un evento che non può più essere visto quale sua mera "conseguenza" naturalistica. L'evento stesso, consumativo del reato può presentarsi con una natura esclusivamente tecnologica.

Diventa complesso individuare l'aspetto volitivo, richiesto per integrare il dolo, necessario per la rimproverabilità al soggetto del reato commesso, essendo la colpevolezza un elemento costitutivo del reato.

Gli effetti del reato si presentano prolungati nel tempo, di fatti si potrebbe operare una distinzione dogmatica fra momento di "perfezione formale" del reato, che si ha quando si realizzano gli elementi costitutivi essenziali e il momento della "consumazione sostanziale" quando il reato ha definitivamente esaurito il suo potenziale di offesa, raggiungendo il massimo grado di lesione del bene giuridico protetto[41].

Per quanto attiene alla persona offesa si evidenziano una serie di asimmetrie, in particolare, una prima osservazione che si impone è l'elevato numero dei casi di perseguibilità a querela nella Legge n. 547[42], il che, se da un lato costituisce il *pendant* rispetto alle corrispettive ipotesi "ordinarie" non considera che nella stragrande maggioranza dei casi l'interessato è del tutto ignaro dell'effettuazione di un illecito ai suoi danni e la tempestiva proposizione della querela risulta perciò particolarmente difficoltosa. A ciò si aggiunga la quasi generalizzata plurioffensività delle fattispecie dei reati informatici, sicché diventa ben difficile la stessa individuazione delle vittime del reato[43].

Infine, diverse posizioni di garanzia si sviluppano in capo a diversi soggetti, come

---

[41] Tale distinzione, accolta nella teoria generale del reato già da F. CARRARA, *Momento consumativo del furto*, in *Lineamenti di pratica legislativa penale*, Torino, 1874, pp. 229 ss.; è recepita nella manualistica italiana e straniera: cfr. F. MANTOVANI, *Diritto penale - Parte generale*, X ed., Padova 2017, pp. 425 ss.; H. JESCHECK, T. WEIGEND T., *Lehrbuch des Strafrechts - Allgemeiner Teil*, V ed., Berlino, 1996, p. 517. Volendo, con riferimento ai reati di dolo specifico, L. PICOTTI*, Il dolo specifico. Un'indagine sugli "elementi finalistici" delle fattispecie penali*, Milano, 1993, pp. 565 ss.

[42] Si intende la prima legge contro la criminalità informatica, ovverosia la L. 21/12/1993, n. 547.

[43] cit. G. CORASANITI, R. PRODI, L. LOEVINGER, *Esperienza giuridica e sicurezza informatica*, Giuffrè, Milano, 2003, pp. 116 e 117.

enti, amministrazioni, imprese, ecc., i quali operano nel *Cyberspace*, attraverso attività potenzialmente pericolose per diritti e interessi giuridici degli utenti e di terzi; perciò, sono tenuti in via preventiva a riconoscere, valutare, circoscrivere i rischi e controllare le fonti da cui derivano, in funzione di prevenzione dei reati e riduzione dei rischi.

Appare evidente l'impatto rivoluzionario che queste nuove tecnologie hanno avuto sul diritto penale. Maturata questa consapevolezza, analizzati tutti gli aspetti che sono stati incisi, si ritiene necessario un adattamento; appare fondamentale per il legislatore e per l'interprete individuare degli schemi di riferimento per ottenere le risposte più adatte al caso concreto, cogliere le analogie e le differenze tra fattispecie contigue, risolvere o prevenire eventuali conflitti tra norme, evitando lacune o sovrapposizioni o incongruenze a livello applicativo e normativo.

### 1.4. *Evoluzione normativa, nell'ordinamento italiano e sovranazionale*

A seguito della Rivoluzione informatica l'intervento normativo è risultato doveroso. In questo capitolo verranno analizzate brevemente le tappe fondamentali dei diversi interventi normativi, costituiti da convenzioni internazionali, direttive europee, regolamenti europei e normative statali interne.

Gli interventi legislativi in Italia sono stati sporadici e settoriali, il legislatore, per prevenire e reprimere la criminalità informatica, è stato notevolmente condizionato dall'azione propulsiva svolta da alcuni organismi internazionali dei quali il nostro Stato fa parte. Specifiche direttive europee hanno dato origine a numerose novelle, soprattutto negli anni Novanta, la più organica risale al 1993 con la L. n. 547/1993; quest'ultima ha integrato le norme del Codice penale e del Codice di procedura penale relative alla criminalità informatica ed era diretta a contrastare le forme "classiche" di manifestazione della criminalità informatica, come ad esempio le frodi e le falsità informatiche.

A livello internazionale un primo importante intervento organico venne attribuito

ad un gruppo di esperti che si riunì a Parigi, per opera del Comitato per la Politica dell'Informazione, dell'Informatica e delle Comunicazioni dell'OCSE[44], e condusse uno studio sulla possibilità di applicare e di armonizzare a livello internazionale le leggi penali per contrastare i reati informatici. Nel 1986 questi studiosi, al termine dei lavori, pubblicarono una relazione contenente l'analisi delle normative esistenti e le proposte elaborate dai vari Stati membri, nella quale raccomandarono l'adozione di una serie di strumenti di natura penale per contrastare i crimini informatici.

In seguito a tale studio il Comitato dei Ministri degli Stati membri dell'OCSE approvò la Raccomandazione n. R. (89) 9[45], in essa si fa riferimento ad una prima catalogazione dei crimini cibernetici, suddivisi in due liste: una indicante le condotte che gli Stati sono invitati a perseguire penalmente (c.d. lista minima); l'altra indicante le condotte da incriminare solo in via eventuale (c.d. lista facoltativa).

Ulteriore passo essenziale è stata la Convenzione sulla Criminalità informatica (*Convention on Cybercrime*) del Consiglio d'Europa del 23 novembre 2001, ratificata ed eseguita in Italia con la L. n. 48/2008; con la quale si cercano di contrastare, applicando norme di diritto processuale e sostanziale, i reati da essa stessa definiti, ma anche a tutti i reati commessi mediante un sistema informatico, nonché a qualsiasi altro reato di cui si debbano o possano raccogliere prove in forma elettronica[46].

A livello comunitario è stata adottata la direttiva 2000/31/CE dell'8 giugno 2000, relativa alla regolamentazione dei servizi informativi ed in particolare del commercio elettronico nel mercato interno; nella quale vennero tracciati dettagliatamente gli elementi identificativi della figura del *Web Service Provider* (prestatore di servizi digitali)[47],

---

[44] vd. OCSE, *Computer-related Crime: Analysis of Legal Policy*, Parigi, 1986.

[45] vd. Counseil De L'Europe, *Recommandation n. R (89) 9*, Strasbourg, passim, 1990. Tale raccomandazione si apre con il riconoscimento dell'importanza di una risposta adeguata e rapida al nuovo fenomeno della criminalità informatica e con la considerazione che la criminalità informatica ha spesso un carattere transfrontaliero.

[46] cfr. Art. 14, comma 2 e art. 23 della Convenzione sulla Criminalità informatica.

[47] L'*Internet Service Provider* ("ISP") è definito come quel soggetto che esercita un'attività imprenditoriale che offre agli utenti la fornitura di servizi inerenti *Internet*, in sostanza è colui che fornisce ai terzi l'accesso alla rete, utilizzando una connessione remota tramite linea telefonica o banda larga (cit. M. IASELLI, *Internet Service Provider, guida all'ISP: cos'è, regime e tipologie di responsabilità*, in *Altalex*, 2019).

spingendosi sino a delinearne gli eventuali profili di responsabilità. Nel 2005 il Consiglio dell'Unione ha emanato la decisione quadro 222/GAI in materia di attacchi informatici a sistemi informativi, con l'intento di migliorare la cooperazione tra le autorità giudiziarie e di polizia degli Stati membri; essa venne poi interamente sostituita dalla Direttiva UE 40/2013. Analizzando i provvedimenti predisposti a contrasto degli attacchi nei confronti dei sistemi informativi, merita di essere ricordata la Direttiva 1146/2016/UE (c.d. NIS), quale strumento di raccordo tra le discipline dedicate alla regolazione del settore pubblico e di quello privato nell'ambito dell'erogazione dei servizi informatici e digitali. Le Istituzioni europee hanno continuato ad adottare misure dirette a rafforzare la sicurezza cibernetica; tra queste ricopre un ruolo primario il c.d. *Cybersecurity Act*, un Regolamento europeo entrato in vigore il 27 giugno 2019, volto all'introduzione di un sistema di certificazione transnazionale di prodotti e servizi digitali, rafforzando al contempo la figura dell'Agenzia dell'Unione Europea per la sicurezza delle reti e dell'informazione[48].

Queste sono alcuni degli interventi normativi adottati a seguito dell'evoluzione tecnologica, la quale è in costante cambiamento; di conseguenza continui saranno anche questi interventi normativi, a livello europeo, nazionale e internazionale, per garantire una sicurezza e una certezza dinanzi ai nuovi problemi che la nostra società deve e dovrà affrontare.

### 1.5. *La nascita del Diritto alla* Privacy

La nostra è una "società digitale" nella quale siamo partecipi di una proliferazione inarrestabile delle connessioni mobili, della progressiva integrazione dei diversi strumenti di comunicazione, dello sviluppo innovativo delle applicazioni tecnologiche. Facciamo

[48] In inglese: *European Network and Information Security Agency* ("ENISA"). Il sui compiti sono: contribuire ad una politica informatica dell'UE, migliorare l'affidabilità dei prodotti, dei servizi e dei processi "TIC" con schemi di certificazione della sicurezza informatica, collaborare con gli Stati membri e gli organismi dell'UE e aiutare l'Europa a prepararsi per le sfide informatiche del futuro.

ricorso quotidianamente ai servizi offerti dalla rete che ci richiedono di poter acquisire le informazioni afferenti la nostra sfera personale.

I nostri dati personali diventano una sorta di "merce di scambio"; vengono raccolti e monitorati costantemente con l'obbiettivo di una profilazione di massa per conoscere gli orientamenti dei consumatori per poi orientarli e influenzarli.

La *privacy* si presenta come un elemento fondante della società ed uno strumento necessario per difendere la libertà e per opporsi alle spinte, sempre più forti, verso la "società della sorveglianza"[49].

Il termine inglese *privacy*, che significa "riservatezza", è diventato di uso comune per indicare la sfera privata di ogni individuo e, in particolare, quell'insieme di informazioni personali sulle quali desideriamo di mantenere il riserbo, escludendone l'accesso ad altri[50].

L'incessante evoluzione dei mezzi tecnologici ha portato la questione *privacy* al centro del dibattito politico, sociale e giuridico degli ultimi decenni. L'identificazione del Diritto alla *privacy* con il diritto alla protezione dei dati personali è il punto di approdo di una lunga evoluzione concettuale, si caratterizza per la sua incessante mutevolezza contenutistica e per la capacità di racchiudere in sé una serie di esigenze multiformi.

La *privacy* nasce con una prima elaborazione teorica nel contesto giuridico statunitense di fine Ottocento; si tratta del *The Right to Privacy*, pubblicato sulla *Harvard Law Review* nel 1890 ad opera di due giuristi di Boston, Warren e Brandeis[51], con la quale affermano l'esistenza, all'interno dell'ordinamento giuridico americano di un autonomo Diritto alla *privacy*, definito come "*the right to be let alone"* ("diritto di essere lasciati in pace"). Il "diritto di essere lasciati in pace" allude essenzialmente alla propria sfera individuale, che dev'essere riservata e protetta come intangibile rispetto agli ingressi

[49] Per approfondire vd. S. ZUBOFF, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Profile Books Ltd, 2018. S. Zuboff, professoressa americana di Harvard, sostiene che le *Big Tech* (società di tecnologia dell'informazione più dominanti) sono determinate a mercificare, controllare e cooptare ogni esperienza umana per trasformarla in un dato comportamentale grezzo da utilizzare per accrescere ancora di più i propri profitti e il proprio potere.

[50] cit. M. ZIZI, Treccani online, in *treccani.it*, 2006.

[51] vd. S. WARREN, L. BRANDEIS, *The right to privacy,* in *Harvard Law Review,* vol. 4, 1890.

abusivi di chiunque[52]. Questa teoria ha trovato piena applicazione all'interno del mondo giuridico europeo ed ha dominato fino a quando le esigenze di una società tecnologicamente avanzata non hanno richiesto una sua ridefinizione.

Nel lungo *iter* evolutivo un ruolo cruciale ha avuto l'opera della giurisprudenza, la quale, dinnanzi all'incertezza della dottrina e al silenzio del legislatore, ha saputo riconoscere la valenza giuridica delle esigenze di tutela della vita privata, sollecitando così il legislatore italiano ad attivarsi per garantire piena ed effettiva tutela al Diritto alla *privacy*.

Dopo un lungo e travagliato processo di riconoscimento, l'iniziale "diritto ad essere lasciati soli" si è trasformato, quindi, nel "diritto alla protezione dei dati personali", inteso quale diritto a che nessuno possa utilizzare informazioni private di un soggetto senza il suo consenso, riconosciuto alla stregua di diritto fondamentale della persona sia dal sistema giuridico nazionale che da quello comunitario. Quindi, in sintesi, tale diritto si esplica sia attraverso la protezione da condotte di aggressione contro la sfera privata, sia con la protezione da condotte di diffusione di informazioni afferenti questa particolare sfera privata.

La riservatezza rappresenta il bene giuridico principale per il quale si costruisce una tutela penale, la cui rilevanza è avvertita dalla collettività che trova riconoscimento anche a livello costituzionale grazie una lettura aperta dell'art. 2 Cost.[53].

Nel contesto giuridico internazionale, da tempo, l'espressione più usata al posto di *privacy* è "*Data protection*" per sottolineare che non si tratta di stare chiusi nel proprio mondo privato, al riparo da sguardi indiscreti, ma anche di potersi proiettare liberamente nel mondo attraverso le proprie informazioni, mantenendo però sempre il controllo sul modo in cui queste circolano e vengono da altri utilizzate[54].

---

[52]cit. L. PICOTTI (a cura di), op. cit., p. 175.

[53] Secondo questa prospettiva l'art. 2 Cost. va letto come una "fattispecie aperta", e alla luce sia dell'art. 12 della Dichiarazione universale dei diritti dell'uomo, ove si sancisce che nessun individuo può essere sottoposto ad interferenze nella sua vita privata; sia dell'art. 8 della Convenzione europea sulla salvaguardia dei diritti dell'uomo e delle libertà fondamentali, secondo cui ogni persona ha diritto al rispetto della vita privata e famigliare.

[54] cit. S. RODOTÀ, *Intervista su Privacy e libertà,* Editori Laterza, 2005, p. 19.

A tal proposito, un'autorevole dottrina[55] ha sottolineato che sia il diritto a mantenere private le questioni della propria sfera personale, sia il diritto a controllare l'uso dei propri dati personali, sono una *condicio sine qua non* l'individuo non ha la libertà di autodeterminazione[56]. La *privacy* diventa una precondizione necessaria per l'esercizio della libertà personale di ciascun individuo, la sua tutela risulta indispensabile, altrimenti si potrebbero verificare discriminazioni ingiustificate, basate sul sesso, sulle proprie idee politiche, sulle proprie credenze religiose e così via.

Il Diritto alla *privacy* può rivestire l'accezione di riservatezza informatica, concetto che allude a: «*quelle nuove aree virtuali ove i soggetti titolari memorizzano ed elaborano con una certa facilità e velocità un'ampia quantità di informazioni e di dati, con conseguente libera valorizzazione della personalità individuale e svolgimento di qualsiasi attività di natura economica, libero-professionale, sociale, culturale* […]. *Dunque, l'ambito di tutela di tale bene giuridico è rappresentato dall'esigenza di salvaguardare il pieno diritto di godimento di tali confini virtuali da parte del legittimo titolare, e ciò si proietta non solo sul contestuale sviluppo della personalità umana, ma prefigura anche la possibilità di escludere soggetti terzi dall'illimitata possibilità di intrusione nel sistema informatico altrui*»[57].

Il legislatore europeo con la direttiva 95/46/CE relativa al trattamento dei dati personali, in Italia recepita con la legge 675/96, ha predisposto una disciplina a tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, con l'obbiettivo di trovare un equilibrio tra il rispetto del diritto alla vita privata e la libera circolazione dei dati tra gli Stati membri, anche attraverso uno standard comune che gli Stati europei sono obbligati a rispettare. I principi della direttiva sono poi stati fatti propri dall'art. 8 della Carta dei diritti fondamentali dell'Unione

---

[55] Come osserva S. RODOTÀ, op. cit., p. 149, cit. «*il concetto di privacy è sempre più legato alla tutela della libertà personale, esistenziale: il diritto di compiere le proprie scelte, di mantenere le proprie caratteristiche, non solo senza subire alcun tipo di discriminazione ma anche senza perdere interi pezzi di identità nei mille meccanismi delle nuove tecnologie*».

[56] Per libertà di autodeterminazione si intende la capacità di scelta autonoma ed indipendente dell'individuo.

[57] cit. M. CASELLATO, A. DI MAIO, D. LA MUSCATELLA, *Il nodo gordiano dello "sviamento di potere" nell'accesso abusivo ad un sistema informatico, tra suggestioni dogmatiche e riflessioni giurisprudenziali*, in *Cassazione penale*, fasc. n. 7, 2019, p. 2780.

europea[58], con una disposizione specifica conferisce al diritto alla protezione dei dati personali una piena autonomia giuridica.

La *privacy* ha raggiunto una piena tutelata sia a livello nazionale che sovranazionale. Preme ricordare, però, che la *privacy* è un concetto che risente fortemente dei mutamenti sociali, culturali e soprattutto tecnologici; quindi, sempre in corso di evoluzione e di definizione. Nonostante gli indubbi meriti, la direttiva si rivelò molto presto inadeguata, per questo venne integrata dal regolamento CE n. 45/2001 e poi abrogata dal Regolamento (UE) 2016/679.

Il regolamento CE n. 45/2001 fu caratterizzato per una novità fondamentale: l'introduzione di una nuova figura, il Garante europeo della protezione dei dati. Il Garante europeo della protezione dei dati è una figura di sorveglianza indipendente vigila sul rispetto del diritto alla vita privata delle persone fisiche nel trattamento dei dati personali da parte degli organi dell'Unione Europea, i quali non possono trattare dati personali relativi all'orientamento politico, sessuale, religioso, filosofico o sindacale, salve naturalmente alcune necessarie eccezioni.

Nel contesto giuridico italiano la questione *privacy* tardò a farsi sentire, solo negli anni Cinquanta del Novecento si iniziò a sviluppare un ampio dibattito dottrinale che trovò causa nella mancanza di una norma esplicita e di portata generale quale fondamento giuridico del diritto alla riservatezza. L'apporto dato dalla giurisprudenza è stato cruciale, il caso cardine "Caso *Soraya Esfandiary*" ha portato al riconoscimento del diritto alla riservatezza come figura giuridica autonoma, la Corte di Cassazione civile, sez. III con la Sentenza n. 2129/1975[59] stabilì: «*Il nostro ordinamento riconosce il diritto alla riservatezza, che consiste nella tutela di quelle situazioni e vicende strettamente familiari e personali le quali, anche se verificatesi fuori del domicilio domestico, non hanno per i*

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

[59] In breve, il fatto: riguardava delle controversie instaurate dalla principessa *Soraya Esfandiary* contro alcuni giornali che avevano pubblicato delle fotografie realizzate con un teleobiettivo che la ritraevano in atteggiamenti intimi con un uomo nelle mura della sua abitazione.

*terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non sono giustificate da interessi pubblici preminenti*». Un'importante svolta si concretizzò con il D. Lgs. n. 196 del 30 giugno 2003, denominato Codice sulla protezione dei dati personali[60], si tratta un'opera di sistemazione e di armonizzazione delle norme vigenti in materia di protezione dei dati personali.

A livello comunitario si approda infine al Regolamento (UE) 2016/679, c.d. *General Data Protection Regulation* (GDPR), il quale regola la raccolta, l'elaborazione e la gestione dei dati personali delle persone all'interno dell'Unione Europea; tra i suoi obbiettivi vi è quello di adeguare la disciplina del trattamento dei dati personali ai nuovi rischi emersi con l'evoluzione tecnologica e imporre delle regole comuni in materia di trattamento dei dati personali, in modo da eliminare la disparità di trattamento tra Stati membri.

Ci si dovrebbe interrogare sul significato stesso del concetto di *privacy.* Per poter dare uno statuto autonomo a detto diritto bisognerebbe dimostrare che l'attuale sistema dei diritti fondamentali non soddisfa tutte le esigenze di tutela dell'individuo. In altri termini, è necessario chiedersi se la *privacy* si possa veramente considerare un diritto autonomo o, come appare più coerente, un "*umbrella word*", cioè una categoria meramente ordinatoria da utilizzare come sintesi del coacervo di diritti (dignità personale, riservatezza delle comunicazioni, inviolabilità del domicilio, libera manifestazione del pensiero) che normalmente le Costituzioni già tutelano e che si associano all'istituto in questione. Sia la vecchia direttiva 95/46/CE, sia il nuovo Regolamento (GDPR), concepiscono la protezione dei dati personali come istituto strumentale alla tutela dei diritti e alle libertà fondamentali dell'interessato. In altri termini, la protezione dei dati personali serve per proteggere anche la *privacy*, ma non le equivale né esaurisce la propria funzione tutelandola[61].

[60] Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) n. 2016/679.

[61] cit. L. LUPARIA [et. al.], A. MONTI (a cura di), *Cybercrime e responsabilità da reato degli enti: prevenzione, modello organizzativo e indagini preliminari*, Giuffrè, Milano, 2022, pp. 226 e 227.

## CAPITOLO II

## GDPR (*GENERAL DATA PROTECTION REGULATION*): EVOLUZIONE ED APPLICAZIONE DELLA DISCIPLINA EUROPEA SULLA *PRIVACY*

SOMMARIO: 2.1. Origine e storia del Regolamento (UE) n. 679 del 2016. – 2.2. I principi generali nel trattamento dei dati personali. – 2.2.1. Principio di liceità, correttezza e trasparenza. – 2.2.2. Principio di limitazione delle finalità. – 2.2.3. Principio di minimizzazione dei dati. – 2.2.4. Principio della limitazione della conservazione. – 2.2.5. Principio di esattezza, aggiornamento e cancellazione dei dati. – 2.2.6. Principio della sicurezza e riservatezza. – 2.2.7. Principio di *accountability*. – 2.3. Le tipologie di dati. 2.3.1. La nozione di dato personale. – 2.3.2. I dati identificativi. – 2.3.3. I dati particolari. – 2.3.4. I dati giudiziari. – 2.3.5. I dati anonimi e pseudonimi. – 2.4. I soggetti coinvolti. – 2.4.1. Il titolare del trattamento. – 2.4.2. Il responsabile del trattamento. – 2.4.3. L'incaricato del trattamento. – 2.4.4. ll DPO, *Data Protection Officer*. – 2.5 I diritti dell'interessato. – 2.5.1. Diritto di accesso. – 2.5.2. Diritto di rettifica e limitazione del trattamento. – 2.5.3. Diritto all'oblio. – 2.5.4. Diritto alla portabilità dei dati. – 2.5.5. Diritto di opposizione. – 2.5.6. Diritto di revocare il consenso. – 2.6. La violazione o la perdita dei dati. – 2.7. Ricorsi e sanzioni. – 2.8. Il trasferimento dei dati verso Paesi terzi o organizzazioni internazionali.

### 2.1. *Origine e storia del Regolamento (UE) n. 679 del 2016*

Il Diritto alla *privacy*, a seguito di un lungo iter evolutivo, venne considerato alla stregua di un diritto fondamentale della persona e come tale da tutelare efficacemente.

Ormai da molti anni, si avverte l'impellente esigenza di proteggere la nostra riservatezza esposta sempre di più, a causa all'avanzare delle nuove tecnologie, ad ingerenze altrui; proprio per questo, a livello europeo è stato adottato il Regolamento

(UE) 2016/679, c.d. GDPR (*General Data Protection Regulation*), volto a garantire sia la protezione dei dati personali[62] sia la loro circolazione.

La regolamentazione della *privacy* è sempre più rigorosa ed è diventata fonte di preoccupazione per le aziende, indipendentemente dal loro settore di operatività, dalle loro dimensioni, dalla loro portata e dall'area geografica in cui si trovano. I requisiti imposti dal Regolamento sulla protezione dei dati personali sono complessi, elaborati e rigorosi per qualsiasi organizzazione o individuo che opera all'interno del territorio dell'Unione Europea.

Inizialmente, venne emanata la Direttiva 95/46/CE[63] in un'epoca in cui *Internet* si trovava in uno stadio iniziale di sviluppo, con il passare del tempo tale direttiva iniziava a presentare una serie di problematiche. Le disposizioni apparivano ormai obsolete, specie considerando la velocità e l'ampiezza della diffusione dei nuovi mezzi digitali di informazione, mancava una legislazione sui dati trattati a fini investigativi e giudiziari; infine, essendo una direttiva si creava una frammentazione statale, le varie disposizioni venivano interpretate ed applicate in modo diverso in ogni Paese. La direttiva venne ugualmente considerata come una pietra miliare, i suoi obiettivi: assicurare il funzionamento del mercato unico e l'effettiva protezione dei diritti e delle libertà fondamentali delle persone fisiche, rimasero comunque validi.

Nel nuovo e dinamico ambiente digitale le norme in essa contenute non permettevano più di realizzare il grado di armonizzazione richiesto, né si caratterizzavano per una sufficiente tutela del diritto alla protezione dei dati personali.

Il 25 gennaio 2012 la Commissione Europea decise di reagire con una proposta di regolamento. Gli obbiettivi in essa contenuti si possono riassumere in: rafforzare i diritti delle persone e il mercato interno dell'UE; garantire un'attuazione più rigorosa delle

---

[62] vd. Definizione di "dato personale" prevista all'art. 4, n. 1) del GDPR: «*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 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*».

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

norme; semplificare i trasferimenti internazionali di dati personali; stabilire norme a livello mondiale in materia di protezione dei dati; cercare di dare ai cittadini un maggiore controllo dei loro dati personali, consentendone un accesso più facile; tutelare le informazioni personali, ovunque esse si trovino; e conferire il potere alle autorità di controllo di irrogare ammende nei confronti delle imprese che non rispettino tali norme.

Trattandosi di un regolamento per la sua adozione si è applicata la procedura legislativa ordinaria prevista agli artt. 288 e ss. TFUE[64]. Il 6 e il 15 aprile del 2016 il Consiglio ed il Parlamento diedero la propria approvazione definitiva al regolamento, pubblicato sulla Gazzetta Ufficiale il 4 maggio del 2016[65].

Ai soggetti tenuti all'adeguamento vennero concessi due anni di tempo per provvedervi, termine decorrente dall' entrata in vigore dell'atto; questa scissione temporale, tra validità ed efficacia del corpo normativo, era evidentemente finalizzata a garantire a tutti i soggetti obbligati un tempo congruo per l'adeguamento ovvero per prepararsi ad esso.

La scelta di adottare un regolamento, anziché una direttiva, ha una ragione ben precisa. Come prima visto, una delle problematiche che ha portato all'abbandono della Direttiva 95/46/CE è stata l'interpretazione e l'applicazione diversificata dei vari Paesi europei, questo perché una direttiva europea si limita a stabilire un obbiettivo che tutti gli Stati membri devono conseguire e per essere applicata dev'essere previamente recepita attraverso un atto di diritto interno; per cui spetta al legislatore nazionale, attraverso tale atto, scegliere i mezzi più adatti al raggiungimento dell'obbiettivo stabilito. Mentre, il regolamento è una fonte di diritto derivato con una portata generale, vincolante in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri; per cui non è

[64] Nella procedura legislativa ordinaria, il Parlamento europeo è co-legislatore con il Consiglio europeo. Tale procedura è stata introdotta dal Trattato di Maastricht, rappresenta ad oggi il metodo maggiormente utilizzato nel processo decisionale dell'Unione Europea. Il funzionamento è descritto in dettaglio nell'art. 294 TFUE, per cui il Parlamento e il Consiglio legiferano su un piano di parità. Le due istituzioni adottano gli atti legislativi in prima lettura o in seconda lettura, se al termine della seconda lettura le due istituzioni non hanno ancora trovato un accordo viene convocato un comitato di conciliazione. Le decisioni vengono adottate da una maggioranza qualificata.

[65] Si tratta del procedimento 2012/0011/COD che ha adottato il documento numero 32016R0679, consultabile su *data.europa.eu*.

necessario un atto di recepimento, le sue norme si applicano senza interposizione di atti legislativi da parte del competente organo statuale[66].

Il regolamento ha permesso di soddisfare l'esigenza di tutela avvertita da tempo, garantendo un'uniformità nell'applicazione dei principi dettati dal legislatore europeo. Di fatto, però, la vincolatività del Regolamento (UE) 2016/679 non è così pervasiva, in alcune parti risulta lacunoso e in altre lascia un certo margine di manovra agli Stati membri; infatti, è lo stesso GDPR a mantenere intatta la competenza legislativa specifica degli Stati membri[67].

La recente normativa introdotta dal GDPR armonizza le disposizioni relative alla tutela dei dati personali in tutti i Paesi dell'Unione; adatta il quadro normativo al nuovo contesto sociale ed economico, caratterizzato da un costante progresso tecnologico e da un'ampia e diffusa circolazione e sfruttamento dei dati; contestualmente, rafforza le garanzie poste a tutela dei dati personali e dei diritti degli individui. Questa operazione di armonizzazione si riscontra anche a livello nazionale con l'emanazione del D. Lgs. del 10 agosto 2018, n. 101 avente l'obbiettivo di adeguare, attraverso una delega al Governo, il quadro normativo nazionale, caratterizzato dal D. Lgs. 196/2003[68], alle nuove disposizioni del Regolamento.

Alla base del Regolamento vi sono due principi cardine che riguardano il trattamento dei dati personali: l'informativa e il consenso[69]. Tali principi garantiscono una piena tutela dei diritti e delle facoltà delle persone fisiche coinvolte. Si tratta di due adempimenti obbligatori, per cui il titolare del trattamento è tenuto a fornire ai soggetti,

---

[66] *Ex* art. 189 del Trattato istitutivo della Comunità Europea il quale qualifica il regolamento come un atto di «*portata generale* […] *obbligatorio in tutti i suoi elementi e direttamente applicabile in tutti gli Stati membri*».

[67] vd. Considerando n. 10 del GDPR: «*Per quanto riguarda il trattamento dei dati personali per l'adempimento di un obbligo legale, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del presente regolamento*».

[68] D. Lgs. 196/2003, c.d. Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) n. 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.

[69] *Ex* artt. 13 e 14 del GDPR.

di cui si appresta a trattare i dati, tutte le informazioni necessarie relative a suddetto trattamento e gli interessati, affinché il trattamento possa essere considerato lecito, devono fornire il proprio consenso.

Il GDPR si occupa di imporre l'adozione di un principio noto negli ambienti della sicurezza informativa come "*need to know*" (necessità di sapere). Chi raccoglie dati personali dev'essere certo di avere titolo per farlo; allo stesso modo, quando li comunica deve accertarsi di avere titolo per consegnarli e che il ricevente abbia titolo per riceverli. Il che spiega la *ratio* alla base degli obblighi di adozione delle misure di sicurezza prescritte; da un lato, il titolare deve evitare che i soggetti non legittimati possano accedere a dati personali il cui trattamento sarebbe loro precluso, dall'altro lato, deve fare in modo che siano trattati esattamente i dati personali riferiti all'interessato e non ad altri o a nessuno[70].

Tra le tante novità si verifica una profonda rivoluzione nell'approccio alla protezione dei dati: le aziende e le istituzioni saranno tenute ad operare in conformità al principio di responsabilizzazione, noto come principio di "*accountability*"[71]. La protezione dei dati non sarà più considerata un mero adempimento formale, ma costituirà un aspetto intrinseco e duraturo delle operazioni aziendali, accompagnato dall'impegno a sensibilizzare gli utenti in merito ai propri diritti e alle proprie libertà. Secondo tale principio il titolare del trattamento dev'essere in grado di dimostrare di aver adottato efficacemente un complesso di misure giuridiche e tecniche dirette alla protezione dei dati[72].

Un'importante innovazione è la completa applicabilità del Regolamento alle

---

[70] cit. L. LUPARIA [et. al.], A. MONTI (a cura di), op. cit., p. 228.

[71] In *Lessico del XXI Secolo*, 2012) l'enciclopedia Treccani definisce "*accountability*": «*in senso ampio, il dovere da parte dei responsabili di un'organizzazione (privata o pubblica), di documentare e rendicontare i risultati raggiunti, i modi in cui sono stati conseguiti e i mezzi utilizzati per il loro raggiungimento nei confronti di uno o più portatori di interessi (ingl. stakeholders) interni od esterni all'organizzazione stessa, al fine di rendere possibile un giudizio di verifica della conformità dei comportamenti adottati rispetto al mandato ricevuto e prevedendo conseguenze positive (premi) o negative (sanzioni) a seconda degli esiti della procedura di verifica*».

[72] cfr. L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale scientifica, Napoli, 2017, e G. FINOCCHIARO, *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017.

aziende situate al di fuori dell'Unione Europea che offrono servizi o prodotti a persone presenti nel territorio europeo ovvero ne monitorano il comportamento.

Ogni utente avrà il diritto di ricevere informazioni chiare e precise sull'utilizzo che ne verrà fatto dei propri dati personali, potrà trasferirli dal titolare del trattamento ad un altro soggetto e godrà di una maggiore tutela per quanto riguarda il diritto di richiedere la cancellazione delle informazioni, non più necessarie rispetto alle finalità per cui sono state originariamente raccolte[73].

Imprese ed enti dovranno rispettare i principi della "*privacy by design*" e della "*privacy by default*"[74], il primo principio fa riferimento all'applicazione, sin dal momento della progettazione e dello sviluppo di sistemi informatici adibiti al trattamento di dati, di misure tecniche e organizzative che risultino efficaci a garantire i principi di protezione dei dati; il secondo principio prevede che il titolare del trattamento scelga, per impostazione predefinita, di svolgere solo i trattamenti di dati personali strettamente necessari a conseguire la specifica e lecita finalità che ha stabilito, nel pieno rispetto dei principi generali di minimizzazione dei dati (non raccogliere più dati del necessario), limitazione delle finalità (non trattare i dati per scopi diversi da quelli stabiliti), e limitazione della conservazione (non mantenere i dati quando non sono più necessari).

Il consenso all'uso dei dati dovrà essere ancora più specifico per ogni servizio reso; dev'essere fornito mediante un "chiaro atto affermativo", frutto di un'azione deliberata dell'interessato[75].

Il titolare del trattamento ha l'obbligo di informare, tempestivamente, le Autorità

---

[73] Ci si riferisce al c.d. "diritto all'oblio" previsto all'art. 17 del GDPR, nasce a seguito della Sentenza della Corte di Giustizia UE, n. 317 del 13 maggio 2014 e prevede la possibilità di richiedere ai motori di ricerca, come *Google*, di rimuovere determinati risultati, relativi ad informazioni personali, se queste risultano "inesatte, inadeguate, irrilevanti o eccessive" ovvero si deve verificare se è di interesse pubblico che tali informazioni restino disponibili nei risultati di ricerca.

[74] *Ex* art. 25 del GDPR, rubricato "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita".

[75] vd. Definizione di "consenso" prevista all'art. 4, n. 11) del GDPR: «*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*».

garanti[76] e i soggetti interessati nel caso in cui si verifichi una violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati[77].

Altra importante innovazione è la figura del *Data Protection Officer* (DPO)[78] che dovrà operare all'interno delle amministrazioni pubbliche e delle imprese per osservare, valutare e organizzare la gestione del trattamento di dati personali, e dunque la loro protezione, affinché questi siano trattati nel rispetto delle normative *privacy* europee e nazionali.

Infine, sono previste anche diverse sanzioni per chi non rispetta le disposizioni, le quali possono comprendere un ammonimento, un divieto temporaneo o definitivo di trattamento e una sanzione pecuniaria fino a 20 milioni di euro, pari al 4% del fatturato totale annuo dell'azienda.

## 2.2. *I principi generali nel trattamento dei dati personali*

### 2.2.1. *Principio di liceità, correttezza e trasparenza*

Il trattamento dei dati personali, secondo quanto previsto dal Regolamento (UE) 2016/679, deve avvenire nel rispetto di una serie di principi. Devono essere applicati il principio di liceità, correttezza e trasparenza secondo quanto previsto all'art. 5, paragrafo 1, lett. a).

Per principio di liceità ci si riferisce alla regola per la quale il trattamento dei dati è sempre vietato, salvo che non ricorra una delle ipotesi previste dal Regolamento all'art. 6, ovvero, le cosiddette "condizioni di liceità". Affinché un trattamento risulti lecito è sufficiente che si verifichi anche una sola di queste condizioni. I fondamenti di liceità

[76] Nel nostro ordinamento, ci si riferisce al Garante per la Protezione dei Dati Personali (GPDP).
[77] La violazione viene anche definita, in inglese, come "*data breach*".
[78] In italiano: Responsabile per la Protezione dei Dati (RDP).

previsti all'art. 6, paragrafo 1, del GDPR si possono riassumere come: consenso espresso; adempimento obblighi contrattuali; interessi vitali della persona interessata o di terzi; obblighi di legge di cui è soggetto il titolare; interesse pubblico o esercizio di pubblici poteri; interesse legittimo prevalente del titolare o di terzi.

Il principio di trasparenza si atteggia come regola generale attuativa della volontà del legislatore europeo di rafforzare la tutela del soggetto debole nel rapporto con il titolare del trattamento. È previsto all'art. 12 del GDPR e sancisce che le modalità di raccolta, utilizzazione, consultazione o, in generale, di trattamento dei dati personali devono essere trasparenti per le persone fisiche interessate. Si impone un'informazione e una comunicazione comprensibili, facilmente accessibili con un linguaggio semplice e chiaro; tale informativa dev'essere inerente all'attività di trattamento, sia rispetto al momento di acquisizione dei dati, sia rispetto alla fase iniziale del trattamento. Infine, corollario del principio in esame è anche la regola generale prevista al paragrafo 5 dell'art. 12 del GDPR ovvero che tutte le informazioni e comunicazioni relative ai diritti dell'interessato devono essere rese gratuitamente.

### 2.2.2. *Principio di limitazione delle finalità*

Il principio di limitazione delle finalità è previsto all'art. 5, paragrafo 1, lett. b) del GDPR, il quale statuisce che i dati personali sono: «*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»)*».

È necessario che le finalità del trattamento dei dati personali debbano essere

esplicite e precisate all'interessato al momento della raccolta dei dati, corollario è che tali finalità debbano essere legittime e che il trattamento risulti compatibile con lo scopo dichiarato.

Nel caso in cui, nel corso del trattamento, sorgano delle nuove e diverse finalità è necessario sottoporre all'interessato una nuova informativa, in modo da ottenere una nuova manifestazione di consenso.

Lo stesso Regolamento stabilisce una serie di finalità ulteriori non incompatibili con le finalità iniziali, che sono: trattamenti a fini di archiviazione nel pubblico interesse, di ricerca scientifica, storica o per fini statistici. Differente è il caso di trattamento ulteriore necessario per salvaguardare importanti obbiettivi di interesse pubblico generale, in questo caso il titolare del trattamento potrà trattare i dati a prescindere dalla compatibilità con le finalità.

In conclusione, è necessario, che il titolare del trattamento indichi possibili reati o minacce alla sicurezza pubblica e trasmetta i dati personali ad un'autorità competente; in questo caso la trasmissione o l'ulteriore trattamento sono vietati se il trattamento non è compatibile con un obbligo vincolante di segretezza di natura giuridica, professionale o di altro genere.

Per di più, secondo quanto disposto all'art. 6, paragrafo 4 del GDPR non è sempre necessaria una totale sovrapposizione tra le finalità inserite nell'informativa rivolta all'interessato e il trattamento effettivamente esperito; purché tali finalità secondarie e diverse rispetto a quelle iniziali, oggetto di informativa, superino il giudizio di compatibilità secondo una serie di criteri stabiliti nel medesimo articolo[79]. In questo modo il titolare del trattamento può, sulla base di un'autonoma valutazione di compatibilità, trattare i dati personali anche per finalità diverse rispetto a quelle per le quali sono stati

[79] *Ex* art. 6, par. 4 del GDPR: «*Il titolare del trattamento tiene conto, tra l'altro: a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto; b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento; c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell' articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell' articolo 10; d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione*».

raccolti, ma sempre mantenendo al centro i diritti e le libertà degli interessati. A tal proposito, il Considerando n. 50 del GDPR garantisce che vi sia un obbligo di informare l'interessato di tali altre finalità e dei suoi diritti, compreso il diritto di opporsi.

### 2.2.3. *Principio di minimizzazione dei dati*

I dati personali oggetto del trattamento devono essere: «*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*», è quanto recita l'art. 5, paragrafo 1, lett. c) del GDPR. Si tratta del c.d. principio di minimizzazione dei dati, secondo il quale possono essere raccolti solo i dati strettamente necessari all'esecuzione dell'incarico.

### 2.2.4. *Principio della limitazione della conservazione*

Secondo il principio della limitazione della conservazione[80] si stabilisce l'obbligo di assicurare un periodo di conservazione dei dati personali limitato al minimo necessario; vale a dire, ad un arco temporale sufficiente per conseguire le finalità per le quali i dati vengono trattati.

Il titolare del trattamento per rispettare tale obbligo deve fissare un termine per la cancellazione dei dati, salva la possibilità di conservarli per periodi superiori qualora siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, e a condizione che siano adottate le misure tecniche e organizzative adeguate alla tutela dei diritti e delle libertà.

[80] *Ex* art. 5, par. 1, lett. e) del GDPR.

### 2.2.5. *Principio di esattezza, aggiornamento e cancellazione dei dati*

Si deve garantire l'esattezza, l'aggiornamento e la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento; devono essere adottate misure ragionevoli affinché i dati personali inesatti siano rettificati o cancellati[81].

### 2.2.6. *Principio della sicurezza e riservatezza*

La sicurezza e la riservatezza dei dati personali sono delineate nel Considerando n. 39 del GDPR, che recita: «*I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento*».

A tal proposito, nascono le c.d. misure di sicurezza, definibili come tutti gli accorgimenti che devono "garantire un livello di sicurezza adeguato al rischio" del trattamento, come previsto all'art. 32, paragrafo 1 del GDPR che individua, in via esemplificativa, una serie di fattispecie idonee[82].

Il livello di tutela richiesto segue il principio di adeguatezza dei mezzi al rischio derivante dal trattamento dei dati; tenendo conto dei rischi che derivano, in particolare, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. Tale tutela si realizza tramite l'adozione di misure di sicurezza unitamente alla possibilità di utilizzare specifici codici di condotta o schemi di certificazione per attestare l'adeguatezza delle misure adottate.

---

[81] *Ex* art. 5, par. 1 lett. d) del GDPR.

[82] Tali fattispecie previste all'art. 32, par. 1 del GDPR sono: «*a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento*».

### 2.2.7. *Principio di* accountability

La normativa comunitaria si innesta su un principio cardine ed innovativo, espressamente disciplinato all'art. 5, paragrafo 2 del Regolamento[83], ovvero il principio di *accountability*.

Il titolare del trattamento deve rispettare tutti i principi prima visti e, secondo questo principio di "responsabilizzazione", dev'essere in grado di comprovare di averli rispettati.

Si tratta di un'importante novità rispetto alla precedente Direttiva[84], benché detto principio era già stato ampiamente previsto e trattato dal Garante europeo con il parere n. 3/2010, non si era ancora giunti ad una sua regolamentazione effettiva. Il GDPR prevede e regolamenta espressamente tale principio che funge da pilastro sul quale interpretare tutte le disposizioni in esso contenute.

Per responsabilizzazione si intende il riconoscimento in capo ai titolari del trattamento dell'obbligo di impiegare tutte le misure tecniche e organizzative adeguate a garantire la protezione dei dati personali degli interessati e, soprattutto, adottare comportamenti proattivi tali da dimostrare di aver concretamente adempiuto all'obbligo in modo da soddisfare gli standard di tutela richiesti dal Regolamento.

In breve, si potrebbe asserire che il termine "*accountability*" sintetizzi insieme tre principi: trasparenza, intesa come accessibilità libera alle informazioni; responsività, ovvero la capacità di essere in grado di rispondere circa le scelte effettuate motivandole; ed infine, la *compliance*[85], che si riferisce al rispetto delle norme ed è intesa sia come

---

[83] *Ex* art. 5, par. 2 del GDPR: «*Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)*». Merita di essere riportato anche il testo inglese non tradotto: «*the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ("accountability")*», perché è opportuno rilevare come la comparazione tra la traduzione italiana e quella inglese sconti una vera e propria distanza "culturale", sul tema dell'*accountability*. Una distanza che rischia, se non tenuta in considerazione, di condurre l'interprete a soluzioni diametralmente opposte, non cogliendo il senso autentico del Regolamento (cit. A. FABERI, *Privilegio contro l'autoincriminazione e accountability. Alcuni profili problematici*, in *Archivio penale* 2021, n. 2, p. 2).

[84] Ci si riferisce alla direttiva 95/46/CE.

[85] In ambito aziendale termine utilizzato con il significato di conformità a una legge (per es. il rispetto delle norme per la tutela del lavoro minorile, o di quelle tributarie, o di quelle che vietano l'emissione di gas tossici in particolari lavorazioni ecc.), a uno standard (per es. standard relativi alla qualità

garanzia della legittimità dell'azione, sia come adeguamento dell'azione agli standard stabiliti dal Regolamento.

Nel settore privato, l'*accountability* individua quel processo di responsabilizzazione destinato a coloro che agiscono in maniera trasparente e conforme ai migliori standard, dando conto delle procedure adottate e delle finalità conseguite nelle proprie attività, realizzando al proprio interno dei meccanismi virtuosi di utilità sociale, ulteriori rispetto al risultato economico[86]. L'obbiettivo di detto principio è di anticipare i presidi di controllo, in modo da evitare i pericoli di fatti illeciti prima della loro verificazione, utilizzando un approccio preventivo.

La concretizzazione del principio di *accountability* determina l'applicazione di due principi basilari: "*privacy by design*" e "*privacy by default*". Tali principi operano in sequenza, il "*data protection by design*" detta le regole per l'acquisizione del dato nel rispetto del Diritto alla *privacy*, mentre il "*data protection by default*" si concentra sul dato già acquisito[87].

Il concetto di "*privacy by default*"[88] si ricollega ai già enunciati principi di minimizzazione e limitazione della conservazione dei dati, per cui le imprese dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e

---

o standard applicati per la certificazione del bilancio), a *best practice* (per es. modalità di comportamento, riconducibili ad associazioni di categoria o a organismi nazionali e internazionali, sui più svariati argomenti, come il sistema della *corporate governance*) e a politiche imprenditoriali (per es. il rispetto del codice etico aziendale che evita regalie a soggetti appartenenti alla pubblica amministrazione, che stabilisce regole precise in campo di assunzione del personale ecc.) (cit. Treccani online, Dizionario di Economia e Finanzia, 2012, in *treccani.it*). Nel linguaggio giuridico, il termine *compliance* non è di immediato posizionamento nel sistema della responsabilità. Originariamente si riferiva, in sintesi, al modo di ottenere o mantenere una certificazione di prodotto o di processo che, però, non avevano una diretta valenza in termini di rispetto della legge prescinde(va) dal possesso di una specifica certificazione, rilevando piuttosto il concreto adempimento agli obblighi normativi. Progressivamente, tuttavia, il legislatore ha mutato approccio e ha iniziato ad attribuire rilevanza alle scelte organizzative e alla loro formalizzazione per determinare il limite oltre al quale si configura una responsabilità (essenzialmente) penale (cit. L. LUPARIA [et. al.], A. MONTI (a cura di), op. cit., p. 238).

[86] cit. A. FABERI, op. cit., p. 3.

[87] Non a caso l'art. 25, par. 2, GDPR parla di "quantità di darti personali raccolti", facendo chiaramente riferimento al dato già in possesso dal titolare ovvero dal responsabile del trattamento.

[88] Per "*default*", come comunemente definito in informatica, ci si riferisce al valore preesistente o preselezionato di un'impostazione configurabile assegnata ad un'applicazione *software*, ad un programma informatico o ad un dispositivo; sono anche chiamate "preimpostazioni" o "impostazioni di fabbrica", specialmente per i dispositivi elettronici (cit. European Data Protection Board, *Guidelines 4/2019 on Article 25*, *Data Protection by Design and by Default,* Version 2.0, Adopted on 20 October 2020).

per il periodo strettamente necessario per raggiungerle. L'art. 25, paragrafo 2 del GDPR stabilisce che: «*Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica*».

Con questo modello ci si riferisce alla scelta di valori di configurazione o di opzioni di trattamento impostati, che influisce sulla quantità di dati personali raccolti, sull'entità di questi, sulla portata del loro trattamento, sul periodo di conservazione e sulla loro accessibilità.

Con il concetto di "*privacy by design*", disciplinato all'art. 25, paragrafo 1 del GDPR[89], si intende un approccio di trattamento dei dati che impone alle aziende l'obbligo di avviare qualsiasi progetto introducendo fin dall'inizio gli strumenti a tutela dei dati personali. In tal modo, si garantisce una protezione dei dati fin dalla fase di ideazione e progettazione del trattamento e si prevengono eventuali problematiche future.

Il titolare del trattamento deve attuare una serie di misure tecniche e organizzative adeguate, come la pseudonimizzazione[90], che attuano i principi di protezione dei dati, integrano nel trattamento le necessarie garanzie e tutelano i diritti degli interessati. Dette misure tecniche e organizzative vengono predisposte in modo dinamico ed elastico,

[89] Ai sensi dell'art. 25, par. 1 del GDPR: «*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati*».

[90] Per "pseudonimizzazione" si intende, ai sensi dell'art. 4, par. 5 del GDPR: «*il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile*».

rendendo possibile fin dal principio l'adattabilità del trattamento alle concrete esigenze dell'interessato.

Nel GDPR suddetto approccio lo si può individuare nella c.d. valutazione d'impatto, anche detta *Data protection impact assessment* (DPIA) di cui agli artt. 35 e ss. del GDPR. Si tratta di una valutazione del rischio di impatti negativi[91] sulle libertà e i diritti degli interessati, anche detto "*risk-based approach*".

In questo modo si predispongono una serie di standard di tutela dei dati prima ancora che gli stessi siano effettivamente sottoposti al trattamento e si richiede un'analisi preventiva e un impegno applicativo da parte dei titolari attraverso una serie di attività specifiche e dimostrabili. Si tratta di una prevalutazione che vale come una sorta di autocertificazione e permette di non passare per una valutazione preventiva del Garante *privacy*, il quale effettuerà un controllo solo successivo.

Se dalla valutazione d'impatto risulta un elevato rischio, il titolare o il responsabile del trattamento dovranno necessariamente rivolgersi al Garante per una consultazione preventiva, prima di realizzare il trattamento[92]; Il Garante dovrà fornire, entro un termine di otto settimane[93] dal ricevimento della richiesta di consultazione, un parere scritto.

Infine, detta valutazione non ha portata generale, ma dovrà essere svolta in una

---

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

[92] *Ex* art. 36 del GDPR.

[93] Termine prorogabile di altre sei settimane, qualora il trattamento comporti particolari complessità.

serie determinata di casi. In proposito, è intervenuto il c.d. *Working Party article 29*[94], che ha stabilito una serie di linee guida nel parere WP248rev.01[95], secondo le quali vi sono casi in cui tale valutazione va ritenuta obbligatoria, una serie di parametri da seguire per tutte le operazioni di trattamento che richiedono una DPIA e, infine, una serie di ipotesi di esonero dall'effettuazione della valutazione.

Non vi è assoluta chiarezza circa le ipotesi di obbligo ovvero di esenzione dalla valutazione d'impatto, qualora sussista un dubbio si raccomanda di effettuarla comunque, in quanto è uno strumento utile che assiste i titolari del trattamento a rispettare la legge in materia di protezione dei dati[96].

È estremamente utile, per chiarire il funzionamento della valutazione di impatto, lo schema dell'Autorità francese per la protezione dei dati, c.d. CNIL[97], attraverso un *software* gratuito e liberamente scaricabile[98], propone una versione guidata della modalità di effettuazione della DPIA tramite delle risposte a specifiche domande che prendono in considerazione il contesto del trattamento, il rispetto dei principi fondamentali degli interessati, i controlli di sicurezza, la valutazione dei rischi e la predisposizione di un piano d'azione.

Connessa al concetto di responsabilizzazione vi è una delle incombenze maggiori per le aziende: la tenuta del c.d. registro dei trattamenti, disciplinato dall'art. 30 del GDPR[99]. Ogni titolare del trattamento o un suo rappresentante devono conservare un

---

[94] Il c.d. *Working Party article 29* o, anche detto *Working Group 29*, era un gruppo europeo composto da rappresentanti dei Garanti nazionali e da un rappresentante della Commissione. È stato istituito con la direttiva 95/46/CE, si è occupato delle questioni relative alla tutela della *privacy* e dei dati personali fino al 25 maggio 2018 (entrata in vigore del GDPR); ad oggi sostituito dal Comitato europeo per la protezione dei dati (EDPB).

[95] Consultabile sul sito *europa.eu.*

[96] Sempre secondo quanto detto dal *Working Party Art. 29* (WP29) nel parere WP248rev.0.

[97] Per CNIL si intende "*Commission nationale de l'informatique et des libertés*", un'autorità amministrativa indipendente francese incaricata di assicurare l'applicazione della legge sulla tutela dei dati personali nei casi in cui si effettuino raccolte, archiviazioni ed elaborazioni di dati personali.

[98] *Software* scaricabile dal sito *cnil.fr*.

[99] *Ex* art. 30 del D. Lgs. 231/2001: «*1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni: a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati; b) le finalità del trattamento; c) una descrizione delle categorie di interessati e delle categorie di dati personali; d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali; e) ove*

registro delle attività di trattamento operate, delle quali sono responsabili personalmente. Si possono individuare due tipologie di registro, il registro delle attività e quello delle categorie di attività, i quali possono essere tenuti in forma scritta ovvero in formato elettronico.

Il registro è uno strumento essenziale allo scopo di disporre un quadro aggiornato dei trattamenti posti in essere all'interno di un'azienda, indispensabile per ogni valutazione. Infatti, come affermato dal Garante: «*la tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali*», serve per dimostrare che per ciascun trattamento il titolare e/o il responsabile ha adottato le misure di sicurezza adeguate a tutelare i diritti e le libertà degli interessati coinvolti.

I contenuti minimi del registro sono fissati nell'articolo 30 del GDPR; tuttavia, niente vieta di inserire ulteriori informazioni se ritenuto opportuno. Inoltre, questa attività di redazione del registro prevede una revisione e un aggiornamento costante, soprattutto qualora si verifichino, nell'azienda o nell'organizzazione, importanti modifiche che influiscono sulle modalità di trattamento dei dati personali.

---

*applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate; f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati; g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1. 2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente: a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati; b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento; c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate; d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1. 3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico. 4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo. 5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10*».

Appare da subito chiaro come questo strumento essenziale risulti essere anche particolarmente gravoso e, di conseguenza, controproducente, soprattutto qualora venisse generalizzato. Si deve considerare il c.d. principio di bilanciamento espresso nel Considerando n. 4 del GDPR, secondo il quale: «*Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità*». Per tale ragione, appare ragionevole l'esenzione dalla tenuta del registro in determinate situazioni: per imprese ed organizzazioni con meno di duecentocinquanta dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato; il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati o dati personali relativi a condanne penali di cui all'articolo 10[100].

La documentazione di *accountability* che ogni azienda ed organizzazione è tenuta a redigere, per garantire di riuscire a dimostrare di gestire e trattare i dati conformemente al dettato normativo, trova la sua sintesi nel cosiddetto Modello Organizzativo *Privacy*, o MOP.

Per MOP si intende un insieme di regole e procedure di tipo preparatorio, che nasce con lo scopo di stabilire in modo organico e compatto le politiche e le procedure interne, al fine di conseguire gli obbiettivi nel rispetto della normativa in materia di protezione dei dati personali e nel rispetto dei diritti degli interessati. Da detto Modello l'ente può trarre tutte le indicazioni relative ai criteri di applicazione della normativa individuandone responsabilità, misure di sicurezza messe in atto e motivazioni per le quali abbia valutato di assumerle. Non si tratta di un documento fine a sé stesso, statico e granitico, bensì rappresenta uno strumento dinamico e di ausilio, fondamentale in caso di ispezioni effettuate dall'Autorità Garante. Nelle organizzazioni a media/alta complessità si rende opportuna la predisposizione di un MOP, affinché possa esprimere tutto il suo potenziale, dev'essere concepito, sin dall'indice, come un "vestito su misura", aderente all'organizzazione. Non a caso, tale documento è visto come una forma di mitigazione in

[100] *Ex* art. 30, par. 5 del GDPR.

grado di soddisfare il principio di *accountability* rappresentando la capacità di dimostrare o meglio "rendicontare" le azioni di responsabilizzazione adottate dall'organizzazione[101].

Non si tratta di un documento obbligatorio, ma nell'ambito del generale principio di a*ccountability*, avere un sistema scritto a cui fare riferimento costituisce un'ottima misura organizzativa di responsabilizzazione. Il fatto che il documento non sia obbligatorio implica la libertà di forma, in merito a lunghezza e contenuti. Tuttavia, trattandosi del modello che dovrebbe rispecchiare l'organizzazione dell'ente, le misure adottate, le procedure scelte, ogni MOP dovrebbe essere unico ed esclusivo. Bisogna redigerlo solo se necessario, ossia se funzionale all'organizzazione dell'ente, in modo da evitare un aggravio delle procedure.

Il MOP si compone delle misure tecniche ed organizzative adeguate *ex* art. 24 del GDPR[102], compresa l'attuazione delle politiche in materia di protezione dei dati volte a dimostrare che i trattamenti effettuati dall'azienda siano conformi alle disposizioni del Regolamento. Dette misure devono essere efficaci nel dimostrare che la loro applicazione permetta il raggiungimento degli obbiettivi del Regolamento.

L'individuazione delle misure tecniche ed organizzative deve tenere altresì conto dei rischi associati ai trattamenti valutandoli in termini di origine, natura, probabilità e gravità. In caso di mancanza dell'applicazione delle misure ovvero in caso di applicazione lacunosa o non efficace, si potrebbero verificare danni di tipo fisico, materiale o immateriale, nei confronti dell'interessato o della stessa organizzazione.

Il MOP e i documenti ad esso allegati costituiscono, un punto di partenza, in continuo aggiornamento; il Modello dev'essere coerente, verificato e aggiornato alla luce dei cambiamenti di contesto interni o esterni all'ente[103] ed anche agli eventuali mutamenti normativi.

Ai fini di una completa attuazione ed efficacia è necessario il coinvolgimento e la

---

[101] cit. M. PEREGO, C. PONTI, *La protezione dei dati personali ed il Modello Organizzativo D. Lgs. 231/2001*, p. 2.

[102] *Ex* art. 24, par. 1 del GDPR: «[…] *il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario*».

[103] Mutamenti che potrebbero consistere, per esempio, nell'introduzione di nuovi trattamenti o nell'adozione di nuove tecnologie o, ancora, nel mutamento dei rischi inerenti alle attività aziendali.

formazione del personale. La redazione del MOP è un'operazione che deve coinvolgere tutto il personale dell'organizzazione, che deve altresì essere oggetto di specifica formazione, perché solo un individuo consapevole, che ha acquisito le giuste competenze, può garantire che i processi aziendali vengano svolti in modo efficace. Oltre ad essere un obbligo specifico introdotto dal Regolamento[104], la formazione costituisce la miglior misura di sicurezza che il titolare del trattamento possa predisporre per la tutela dei dati, sia in termini di organizzazione, sia in termini di sicurezza informatica e capacità di riconoscere le minacce in modo autonomo.

In sintesi, il MOP appare essere uno strumento ideale per la documentazione del sistema di gestione della protezione dei dati personali trattati dall'ente di riferimento.

## 2.3. *Le tipologie di dati personali*

### 2.3.1. *La nozione di dato personale*

Ai sensi dell'art. 4, paragrafo 1 del GDPR, per "dato personale" si intende: «*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*».

Tale nozione è riconducibile a tutte quelle informazioni concernenti una persona fisica, ad esempio il nome, il codice fiscale, il numero telefonico, che in ogni caso rendono il soggetto identificato o identificabile; si nota come alcuni di questi dati non sono propri

[104] *Ex* art. 29 del GDPR: «*Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai dati personali non può trattare tali dati se non è istruito in tal senso dal titolare, salvo che lo richieda il diritto dell'Unione o degli Stati membri*».

solo delle persone fisiche, ma possono riferirsi anche alle persone giuridiche; infatti, qualsiasi ente o impresa ha un indirizzo e un numero di telefono.

La nozione giuridica di dato personale dev'essere riferita al contesto, perché anche se un'informazione isolata non è in grado di portare all'identificazione di un individuo, il fatto che detta informazione possa essere utilizzata per l'identificazione tramite incrocio con altri dati, ne determina la natura di dato personale[105].

Il nuovo Regolamento europeo sulla protezione dei dati aggiorna alcune definizioni: i dati sensibili vengono sostituiti dalla dicitura "dati particolari"; vengono introdotte tutele particolari per i dati biometrici e i dati genetici; inoltre, il metodo di trattamento cambia a seconda della categoria dei dati interessati. Per comprendere queste innovazioni è opportuno effettuare un elenco, anche se non esaustivo, delle categorie di dati tutelati.

### 2.3.2. *I dati identificativi*

Il concetto di "dato identificativo"[106] si riferisce ad un'informazione che permette di identificare l'interessato persona fisica.

Si può ravvisare una prima distinzione: dati identificativi diretti e dati identificativi indiretti. Per dati identificativi diretti si intendono quei dati comuni che permettono di identificare direttamente, senza la necessità di incrociarli con altre informazioni, la persona fisica; in via esemplificativa, fanno parte di questa categoria, i dati anagrafici e le fotografie. Mentre, per dati identificativi indiretti ci si riferisce a dati che identificano una persona fisica solo se associati ad altre informazioni, vi rientrano, per esempio, il codice fiscale e l'indirizzo IP[107].

---

[105] cit. M. MARTORANA, A. TESORO, A. BARBERISI (a cura di), *Gdpr: guida pratica agli adempimenti privacy*, CEDAM, 2018, p. 11.

[106] O anche detto "dato comune".

[107] Per indirizzo IP, dall'inglese *Internet Protocol address*, si intende un codice numerico usato da tutti i dispositivi (*computer*, *server web*, stampanti, *modem*) per navigare in *Internet* e per comunicare in una rete locale. Un indirizzo IP costituisce quindi la base per una trasmissione corretta delle informazioni dal mittente al ricevente.

Il titolare del trattamento per raccogliere questi dati deve rispettare il requisito della liceità, ovvero deve avere un motivo comprovato per raccoglierli osservando tutte le prescrizioni riguardanti la prestazione del consenso e le finalità della raccolta.

### 2.3.3. *I dati particolari*

Un'altra categoria è rappresentata dai "dati particolari", disciplinati all'art. 9 del GDPR[108], per i quali è riservato un trattamento speciale. Il legislatore europeo con tale categoria si riferisce a tutti quei dati la cui tutela ha lo scopo di garantire la libertà di pensiero e di opinione, la dignità della persona e la libertà da possibili discriminazioni.

Rientrano in questa categoria anche i dati genetici, i dati biometrici, se utilizzati per identificare in modo univoco una persona, e i dati relativi alla salute[109].

Come anticipato tali dati sono sottoposti ad un trattamento speciale, nel senso che il loro trattamento è sempre vietato, come regola generale, salve le specifiche eccezioni elencate dal secondo paragrafo dell'articolo 9 del GDPR[110].

---

[108] Ai sensi dell'art. 9, par. 1 del GDPR: «*È vietato trattare dati personali che rivelino origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*».

[109] Per "dati genetici" si intendono i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione (*ex* art. 4, n. 13 del GDPR). In particolare, dall'analisi dei cromosomi, dell'acido desossiribonucleico (DNA) o dell'acido ribonucleico (RNA), ovvero dall'analisi di un altro elemento che consenta di ottenere informazioni equivalenti (*ex* Considerando n. 34 del GDPR). Per "dati biometrici" si intendono i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici (*ex* art. 4, n. 14 del GDPR). Infine, per "dati relativi alla salute" si intendono i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute (*ex* art. 4, n. 15 del GDPR).

[110] *Ex* art. 9, par. 2 del GDPR: «*Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: a)l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1; b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie*

La regola generale impone perciò una completa tutela della persona sia nella sua fisicità che nella sua interiorità; tuttavia, il divieto non è assoluto, sono state introdotte numerose e necessarie eccezioni.

### 2.3.4. *I dati giudiziari*

Anche la categoria dei "dati giudiziari", relativi alle condanne penali e ai reati, disciplinata all'art. 10 del GDPR[111], è sottoposta ad una specifica tutela secondo la quale il trattamento deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il

*appropriate per i diritti fondamentali e gli interessi dell'interessato; c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato; e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali; g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato*».

[111] *Ex* art. 10 del GDPR: «*Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica*».

trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

### 2.3.5. *I dati anonimi e pseudonimi*

Come già visto nell'analisi dei principi alla base del trattamento, il Regolamento prevede che i dati debbano essere conservati per un periodo di tempo limitato e non oltre il tempo necessario per raggiungere lo scopo alla base, nel caso in cui il titolare volesse mantenere i dati per un periodo superiore dovrà procedere alla loro anonimizzazione.

Si definiscono "dati anonimizzati" quei dati che sono stati privati di tutti gli elementi identificativi. Tali dati non sono più ritenuti personali perché non risultano più associabili ad una persona fisica o giuridica; perciò, non ricadono più sotto la tutela del GDPR, bensì saranno soggetti alle disposizioni riguardanti la sicurezza dei dati aziendali generici. Attraverso la procedura di anonimizzazione si tutelano le persone e contemporaneamente si sgravano i soggetti titolari del trattamento da pesanti responsabilità nei confronti degli interessati[112].

Un caso a sé è la situazione nella quale alcuni dati, una volta esaurito lo scopo del trattamento, debbano comunque essere conservati per fini statistici, storici o scientifici, per cui non si applicherà tale anonimizzazione, ma delle adeguate misure contro possibili abusi.

Differente è la categoria dei "dati pseudonimi" i quali sono stati artificiosamente modificati negli elementi identificativi con elementi ulteriori e diversi, tali da rendere estremamente difficoltosa l'identificazione della persona fisica interessata. Quindi, si assegna un identificativo in codice (numerico, alfabetico o alfanumerico) all'interessato, in questo modo nessuno può risalire alla sua identità, tranne il titolare del trattamento, il

[112] A tal proposito, l'articolo 3 del decreto legislativo del 30 giugno 2003, n. 196, afferma che: «*I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità*».

quale detiene lo strumento di "decodificazione" che permette di associare i dati alla persona fisica. Sono dati personali perché consentono, seppur indirettamente, l'identificazione del soggetto.

### 2.4. *I soggetti coinvolti*

I soggetti rilevanti in materia di *privacy* sono definiti all'art. 4 del GDPR come: titolare del trattamento, responsabile del trattamento, destinatario e terzo.

Affinché sia pienamente rispettato il Regolamento è necessario che queste figure siano chiaramente individuate, come espressamente stabilito dall'art. 30, paragrafo 1 e paragrafo 2, lett. a) del GDPR[113].

Vi sono poi altri soggetti possono essere coinvolti nel trattamento: l'incaricato al trattamento[114]; l'interessato[115]; il rappresentante; il contitolare, inteso quale titolare del trattamento che opera nel medesimo trattamento in cui opera un altro titolare, definito

[113] *Ex* art. 30, par. 1, lett. a) del GDPR: «*Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni: a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati*». *Ex* art. 30, par. 2, lett. a): «*Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente: a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati*».

[114] L'incaricato al trattamento viene indirettamente previsto all'art. 4, par. 10 del GDPR come: «*le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile*».

[115] L'interessato si può definire come soggetto passivo, i cui dati personali sono oggetto del trattamento.

all'art. 26, paragrafo 1 del GDPR[116]; infine, vi è anche la figura specializzante del *Data Protection Officer*, anche detto DPO[117].

I soggetti si possono suddividere in due macrocategorie: i soggetti attivi e i soggetti passivi. Nella prima categoria vi rientrano il titolare, l'incaricato, il responsabile, il rappresentante e il DPO; mentre, nella seconda categoria vi rientra il soggetto interessato, ossia il soggetto i cui dati personali vengono trattati da parte dei suddetti soggetti attivi, è importante individuarlo in quanto è colui che potrà far valere i diritti riconosciuti dalla normativa.

In breve, il titolare del trattamento[118] determina le finalità e i mezzi del trattamento di dati personali; il responsabile del trattamento[119] tratta i dati personali per conto del titolare; il destinatario[120] riceve comunicazione dei dati personali; infine, il terzo[121] non è né l'interessato, né il titolare, né il responsabile e nemmeno il soggetto autorizzato al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

---

[116] *Ex* art. 26, par. 1 del GDPR: «*Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati*».

[117] Previsto all'art. 37 del GDPR.

[118] *Ex* art. 4, par. 7 del GDPR il titolare del trattamento è: «*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri*».

[119] *Ex* art. 4, par. 8 del GDPR il responsabile del trattamento è: *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*».

[120] *Ex* art. 4, par. 9 del GDPR il destinatario è: «*la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento*».

[121] *Ex* art. 4, par. 10 del GDPR il terzo è: «*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile*».

### 2.4.1. *Il titolare del trattamento*

Il titolare del trattamento[122] viene definito all'art. 4, paragrafo 7 del GDPR come: «*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*».

Pertanto, il titolare del trattamento è l'azienda, il professionista, la Pubblica Amministrazione a cui l'interessato affida i suoi dati personali.

Ha il compito di decidere riguardo alle finalità del trattamento, le modalità di trattamento, gli strumenti da impiegare, le misure di sicurezza e le competenze dei soggetti coinvolti. Rispetto a tali scelte risponde direttamente nei confronti dell'interessato, nel caso in cui i dati raccolti siano oggetto di trattamento illecito o non conforme alla normativa. In poche parole, si tratta della figura che decide il "perché" e il "come" i dati personali debbano essere trattati.

Il Regolamento descrive nel dettaglio, i suoi obblighi e le sue responsabilità, che consistono di fatto nell'implementare politiche adeguate al fine di garantire un livello di sicurezza dei dati conforme al regolamento e nel poterlo dimostrare.

La responsabilità che ricadono su questo soggetto è stabilita all'art. 24 del GDPR[123] il quale delinea il percorso che il titolare dovrà seguire nella determinazione delle finalità e dei mezzi di trattamento affinché sia conforme ai principi del Regolamento.

Il titolare del trattamento dovrà effettuare una mappatura dei trattamenti realizzati;

---

[122] Anche detto, in inglese "*Data controller*".

[123] Art. 24 del GDPR, rubricato "Responsabilità del titolare del trattamento", dispone: «*1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario. 2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento. 3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento*».

individuare possibili rischi connessi al trattamento, effettuando al contempo una valutazione sulle probabilità e sulla gravità di danno che ne possa derivare ai diritti e alle libertà degli interessati; predisporre misure tecniche ed organizzative adeguate per garantire un livello di sicurezza pari al rischio; redigere un *report* per poter rendicontare le decisioni assunte in materia di trattamento dati; infine, riesaminare costantemente le misure di sicurezza adottate procedendo all'aggiornamento della relativa documentazione.

Al fianco del titolare vi può essere la figura del contitolare, si vede all'art. 4, paragrafo 7 del GDPR che le finalità e i mezzi del trattamento possono essere determinati dal titolare singolarmente o insieme ad altri e all'art. 26 del GDPR che dispone: «*Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento*». Il titolare e il contitolare si dividono autonomamente i compiti, anche se ciascun contitolare rimane egualmente responsabile nei confronti dell'interessato.

Affinché si possano facilmente individuare le singole responsabilità dei contitolari, il Regolamento prevede che i rispettivi ruoli siano definiti mediante accordo interno che dev'essere trasparente, a disposizione dell'interessato, deve garantire l'esercizio dei diritti dell'interessato e stabilire quale dei contitolari e in che forma dovrà provvedere a fornire le informazioni di cui agli artt. 13 e 14 del GDPR[124].

In questo caso, perciò, nella definizione delle finalità e dei mezzi di trattamento dei dati personali si avrà una codecisione, in un'ottica di responsabilizzazione.

Per concludere, ai sensi dell'art. 27 del GDPR, se il titolare del trattamento sia stabilito al di fuori dell'Unione europea, ma offra beni e servizi ovvero monitori il comportamento di individui stabiliti al suo interno, egli è obbligato a nominare un rappresentante, il quale deve essere stabilito in uno degli Stati ove avviene il trattamento. Questo rappresentante funge da interlocutore per tutte le questioni attinenti al trattamento, salve le azioni legali che potrebbero essere intraprese contro il titolare o il responsabile originari.

[124] *Ex* art. 26, par. 1 del GDPR.

### 2.4.2. *Il responsabile del trattamento*

Il responsabile del trattamento è un'altra figura cardine disciplinata all'art. 4, paragrafo 8 del GDPR come: «[…] *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*» e ripresa all'art. 28, paragrafo 1 del GDPR nel quale si prevede: «*Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*».

Come prima visto, la responsabilità ricade sul titolare del trattamento, soggetto designato sulla base della posizione che ricopre nell'ente o nell'azienda che tratta i dati, e non in base alle sue specifiche competenze nel campo. Per questo è stata introdotta la figura del responsabile, una figura professionale specializzata nel trattamento dei dati. Quindi, in breve, mentre il titolare è definito dalle responsabilità, il responsabile è definito dalla preparazione tecnica.

Il titolare del trattamento, prima di procedere al conferimento dell'incarico, deve necessariamente accertarsi che il soggetto abbia condotto un'analisi dei rischi interna ed abbia predisposto idonee misure di sicurezza, tali da consentirgli di espletare in mandato garantendo un livello di sicurezza conforme agli standard richiesti dalle disposizioni europee.

Nell'analisi dei rischi verranno individuati una serie di elementi, quali: la tipologia dei dati trattati, le finalità, le categorie di soggetti interessati; successivamente, il fattore rischio verrà correlato con la natura delle operazioni che dovranno essere effettuate su quei dati. Infine, sulla base di queste premesse il titolare si accerterà che il soggetto che intende nominare come "*data processor*"[125] adotti le misure tecniche e organizzative idonee a trattare i dati conformemente alle istruzioni del titolare, garantisca la riservatezza dei dati, fornisca ai soggetti incaricati del trattamento una corretta formazione sulle

[125] In italiano: "responsabile del trattamento".

modalità di trattamento, utilizzi materiali, prodotti, applicazioni o servizi progettati nel rispetto del "*data protection by design*" ed impostati per assicurare "*data protection by default*".

Secondo quanto previsto dall'art. 28, paragrafo 3 del GDPR[126] vi dev'essere un contratto, o un altro atto giuridico, che disciplini in modo specifico e dettagliato gli obblighi del responsabile del trattamento attraverso una serie di clausole[127].

---

[126] *Ex* art. 28, par. 3 del GDPR: «*I trattamenti da parte di un responsabile del trattamento sono Disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento: a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico; b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza; c) adotti tutte le misure richieste ai sensi dell'articolo 32; d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento; e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III; f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento; g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati*».

[127] *Ex* art. 28, par. 3 del GDPR: «*I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento: a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico; b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza; c) adotti tutte le misure richieste ai sensi dell'articolo 32; d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento; e) tenendo conto della natura del trattamento, assista il titolare del*

Il rapporto che si crea tra responsabile e titolare del trattamento è di natura collaborativa; a riprova di ciò vi è un obbligo del responsabile di segnalare eventuali "*data breach*"[128] al titolare, questo sul presupposto che collabori attivamente, comunicando tempestivamente al titolare eventuali violazioni, affinché il titolare possa rispettare l'obbligo di segnalazione al Garante, da adempiere entro 72 ore dalla conoscenza del titolare della violazione.

Questa figura, oltre ad essere responsabile in caso di violazione degli obblighi contrattuali, è direttamente coinvolta nella procedura penale in caso di irregolarità. In particolare, da ricordare, il Considerando n. 79 del GDPR afferma che: «*La protezione dei diritti e delle libertà degli interessati così come la responsabilità generale dei titolari del trattamento e dei responsabili del trattamento, anche in relazione al monitoraggio e alle misure delle autorità di controllo, esigono una chiara ripartizione delle responsabilità ai sensi del presente regolamento, compresi i casi in cui un titolare del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente con altri titolari del trattamento o quando l'operazione di trattamento viene eseguita per conto del titolare del trattamento*».

Tale disposizione sembrerebbe porre un'eccezione a quanto previsto dall'art. 24

---

*trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III; f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento; g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati*».

[128] Per "*data breach*" si intende: «*Una violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*», (cit. in *garanteprivacy.it*). Si può suddividere, secondo il parere del *Working Party ex* art. 29, in: *confidentialy breach,* è il caso dell'accesso non autorizzato a dati personali, con potenziale divulgazione degli stessi; *availability breach,* si verifica quando i dati personali colpiti dall'attacco vengono alterati; *integrity breach,* comporta la modifica dei dati personali.

del GDPR, secondo cui l'esclusivo responsabile è il titolare del trattamento. Si richiede una ripartizione delle responsabilità, ma senza, di fatto, introdurre la possibilità per il titolare di delegare parte della sua responsabilità in ordine alla definizione delle finalità e dei mezzi di trattamento che, a prescindere da qualsiasi contratto, è ad esso attribuita.

Il Considerando n. 79 del GDPR dev'essere letto in combinato disposto con l'art. 82, paragrafo 2 del GDPR il quale prevede che: «*Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento*».

Il titolare sarà responsabile tutte le volte in cui da un trattamento sia derivato un danno ai diritti e alle libertà degli interessati, salva la dimostrazione che l'evento dannoso non gli è in alcun modo imputabile[129]; mentre, il responsabile risponderà unicamente nel caso in cui realizzi attività in violazione delle disposizioni del Regolamento o delle direttive impartite dal titolare.

Infine, viene data la possibilità, ai sensi dell'art. 28, paragrafo 2 del GDPR[130], al responsabile di nominare un altro responsabile, c.d. sub-responsabile, a due condizioni: autorizzazione scritta del titolare e stipula di un contratto o di un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri tra responsabile e sub-responsabile.

Secondo quanto dispone il paragrafo 4 del medesimo articolo[131], il

---

[129] *Ex* art. 82, par. 3 del GDPR: «*Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile*».

[130] *Ex* art. 28, par. 2 del GDPR: «*Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche*».

[131] *Ex* art. 28, par. 4 del GDPR: «*Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure*

sub-responsabile deve rispettare i medesimi obblighi contrattuali in materia di protezione dei dati personali che legano il titolare al primo responsabile.

Nei casi in cui detto soggetto risulti inadempiente il responsabile iniziale conserva l'intera responsabilità nei confronti del titolare, anche ai fini del risarcimento di eventuali danni; purché non venga dimostrati che l'evento dannoso non gli è un alcun modo imputabile[132].

### 2.4.3. *L'incaricato del trattamento*

L' incaricato del trattamento dei dati personali è una figura non espressamente prevista dal Regolamento (UE) 2016/679, ma la sua nomina non risulta incompatibile con le disposizioni dello stesso, anzi appare doverosa nelle realtà nelle quali si trattano ingenti quantità di dati personali. Si tratta di un soggetto che opera sotto la diretta autorità del titolare o del responsabile e si deve attenere alle istruzioni da essi impartite.

Nel rispetto del principio di minimizzazione del trattamento dei dati personali, è fondamentale l'individuazione specifica dei compiti che l'incaricato del trattamento dovrà espletare e delle categorie di dati personali a cui l'incaricato può avere accesso; questo per impedirli di accedere a dati personali, raccolti dal titolare, non strettamente necessari e pertinenti alle mansioni che lo stesso è chiamato ad espletare.

*tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile*».

[132] *Ex* art. 82, par. 1 e 3 del GDPR.

### 2.4.4. *Il DPO*, Data Protection Officer

Una delle principali novità apportate dal Regolamento è l'inserimento della figura del *Data Protection Officer*, anche detto DPO[133], si tratta di un soggetto che svolge funzioni di supporto e controllo, consultive, formative ed informative relativamente all'applicazione del Regolamento"[134].

Questa figura nasce dall'esigenza di affiancare al titolare del trattamento un soggetto dotato di una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del Regolamento[135].

L'art. 37, paragrafo 5 del GDPR stabilisce che il DPO debba essere: «*designato in funzione delle qualità professionali* […] *e delle capacità di assolvere i compiti*». Quindi, è essenziale per ricoprire tale carica, benché non siano previste specifiche attestazioni formali o iscrizioni ad appositi albi, detenere un'approfondita conoscenza della normativa e delle prassi in materia di *privacy*[136].

Si richiede altresì che il DPO conosca le procedure amministrative che caratterizzano il settore specifico di riferimento, in particolare, dovrà: avere una cognizione diretta di tutti i processi aziendali che comportano il trattamento di dati personali; possedere specifiche competenze informatiche, per affiancare il titolare nelle decisioni; fornire idonea consulenza sulla verifica di conformità del sistema elettronico ai principi di *data protection*, previa verifica dell'idoneità delle misure di sicurezza tecniche e organizzative; infine, assicurare i necessari livelli di sicurezza e riservatezza dei dati.

La nomina del DPO non è sempre obbligatoria, ma il Garante sottolinea che, in

[133] In italiano: "Responsabile della protezione dei dati", c.d. RPD.
[134] cit. Garante della *privacy*, doc. *web* n. 8036793, pubblicato il 26 marzo 2018.
[135] *Ex* Considerando n. 97 del GDPR.
[136] vd. Le FAQ per gli Ordini degli Avvocati in materia di protezione dei dati personali, pubblicate dal Consiglio Nazionale Forense il 28 marzo 2018. Sottolineano come la qualifica di DPO possa essere ricoperta, attraverso un contratto di servizi, da un avvocato, il quale ha per peculiarità proprie della professione forense caratteristiche e doveri, in particolare, la segretezza e la riservatezza, propri dello stesso DPO.

ogni caso, si tratta di una figura raccomandata, anche alla luce del principio cardine di *accountability*.

La designazione è obbligatoria nei casi tassativamente individuati dall'art. 37, paragrafo 1 del GDPR, secondo cui: «*a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico*[137]*, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; b) le attività principali del titolare o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico*[138] *degli interessati su larga scala*[139]*; oppure c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10*».

Le lett. b) e c) del suddetto articolo introducono dei concetti non del tutto chiari. Il concetto di "larga scala", richiesto alla lettera b), non trova una definizione specifica all'interno del Regolamento, il quale prevede semplicemente al Considerando n. 91 che i trattamenti di "larga scala" attengono: «*ad una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale*», senza individuare una soglia positivamente quantificabile. Per sopperire a tale incertezza, oltre alla definizione contenuta nel parere 243/2016 del WP29, il Garante, nelle FAQ sul Responsabile dei

[137] Con il parere 243/2016 il WP29 ha chiarito che sono autorità pubbliche o organismi pubblici le autorità nazionali, regionali e locali ma, a seconda del diritto nazionale applicabile, la nozione ricomprende anche tutta una serie di altri organismi di diritto pubblico.

[138] Ancora con parere 243/2016 del WP29 cerca di dare un significato al "monitoraggio del comportamento di detti interessati" che individua in tutte le forme di tracciamento e profilazione su *Internet* anche per finalità di pubblicità comportamentale, siano esse *online* od *offline*. Prosegue chiarendo che "regolare" significa: 1) che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito; 2) ricorrente o ripetuto a intervalli costanti; 3) che avviene in modo costante o a intervalli periodici. Definisce anche "sistematico", che significa: 1) che avviene per sistema; 2) predeterminato, organizzato o metodico; 3) che ha luogo nell'ambito di un progetto complessivo di raccolta di dati; 4) svolto nell'ambito di una strategia.

[139] Sempre con il parere 243/2016 il WP29 riconosce le difficoltà nel definire il concetto di "larga scala", cerca di dargli un significato attraverso una serie di parametri: 1) il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; 2) il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; 3) la durata, ovvero la persistenza, dell'attività di trattamento; 4) la portata geografica dell'attività di trattamento.

dati[140], ha elencato, a livello esemplificativo, quali soggetti possono rientrare in tale figura; si trovano, per esempio: gli istituti di credito, le imprese assicurative, i sistemi di informazione creditizia. In tutti gli altri casi, quali ad esempio: liberi professionisti operanti in forma individuale, agenti, rappresentati e mediatori operanti su larga scala, imprese individuali o familiari ecc., l'obbligo di nomina non risulterebbe operante.

Il DPO viene nominato da ogni titolare o responsabile del trattamento quando ricorrono le ipotesi prima viste ovvero, se queste non ricorrono, nei casi in cui tali soggetti decidano volontariamente di nominarlo.

Il GDPR chiarisce all'art. 37, paragrafo 2 che il DPO dev'essere "facilmente raggiungibile[141] da ciascun stabilimento", nel senso che dev'essere in grado di svolgere le sue mansioni efficientemente, soprattutto quando opera con più committenti.

L'art. 37, paragrafo 6 del GDPR chiarisce che il *Data Protection Officer* può essere un dipendente oppure può assolvere ai suoi compiti in base ad un contratto di servizi.

Dev'essere tempestivamente e adeguatamente coinvolto in tutte le questioni inerenti alla protezione dei dati personali[142]. In base alla natura del rapporto di lavoro, se il DPO è un dipendente allora il titolare o il responsabile del trattamento dovrà richiedere, ovvero ordinare, al DPO di attivarsi nelle questioni di *privacy*; viceversa, qualora sia autonomo, dette modalità, almeno in chiave di regolamentazione generale, dovranno essere individuate nel contratto di servizio.

Il rapporto che lega questi soggetti si basa su di una leale collaborazione, il titolare o responsabile del trattamento devono sostenere il responsabile per la protezione dei dati nell'esecuzione dei suoi compiti, fornendogli le risorse necessarie per adempierli[143].

I compiti nello specifico affidati al DPO sono previsti all'art. 39 del GDPR, in

[140] Consultabili sul sito *garanteprivacy.it*.

[141] Il WP29 chiarisce che per "facile reperibilità" deve intendersi la prontezza delle possibilità di comunicazione da parte degli interessati, dell'autorità di controllo e dei soggetti interni all'organismo o all'ente; tutti devono poter rintracciare il DPO senza difficoltà e senza perdita di tempo.

[142] *Ex* art. 38, par. 1 del GDPR.

[143] *Ex* art. 38, par. 2 del GDPR.

breve sono: fornire consulenza relativamente agli obblighi derivanti dalle disposizioni comunitarie; sorvegliare l'adempimento di tali obblighi da parte dei soggetti coinvolti nel trattamento, assicurandosi che gli stessi siano adeguatamente formati e responsabilizzati sulle misure da adottare; cooperare con l'autorità di controllo, per fungere da punto di contatto tra la stessa e il titolare del trattamento.

Inoltre, al DPO è consentito svolgere altri compiti e funzioni, purché il responsabile o il titolare del trattamento assicuri che tali compiti e funzioni non diano adito ad un conflitto di interessi[144].

I compiti devono essere svolti con terzietà e incondizionalità; per rimanere indipendente il DPO non deve ricevere alcuna istruzione su come assolvere alle proprie funzioni e deve poter fornire la sua opinione dissenziente direttamente al titolare o al responsabile, senza che gli stessi possano disporre la sua rimozione o penalizzazione per aver agito in adempimento. Sarà il titolare del trattamento ad adattare la propria organizzazione in base all' esigenze di questo soggetto.

Inoltre, tra le indicazioni fornite dal Garante si sconsiglia agli enti pubblici di grandi dimensioni, con trattamenti di dati particolarmente complessi e sensibili, di assegnare al DPO ulteriori responsabilità connesse alla ordinaria attività dei singoli uffici interni; questo perché si rischierebbe sull'effettivo svolgimento dei compiti attribuiti al DPO.

Il *Data Protection Officer*, ai sensi dell'art. 38, paragrafo 5 del GDPR, è tenuto al segreto e alla riservatezza in merito all'adempimento dei propri compiti; quindi, non può rivelare le informazioni che riguardano l'impresa e la sua organizzazione di cui viene a conoscenza e le informazioni riferibili a terzi, i cui dati vengono trattati.

Il DPO non è personalmente responsabile in caso di inosservanza degli obblighi in materia di protezione dei dati personali, perché spetta al titolare del trattamento o al responsabile del trattamento garantire di dimostrare che il trattamento è effettuato conformemente al Regolamento; perciò, la responsabilità ricade sul titolare o sul responsabile del trattamento, salvo prova contraria.

[144] *Ex* art. 38, par. 6 del GDPR.

Il coinvolgimento del DPO nella vita dell'organizzazione, sotto il profilo della protezione dei dati personali, si esplica anche attraverso il confronto con altri Organi di controllo. Il DPO, consapevole che gli Organi di controllo trattano dati per svolgere le attività ad essi affidate, intrattiene con loro rapporti in maniera continuativa e rendicontata. Non può sussistere alcun conflitto di interesse tra il DPO e detti soggetti. Il DPO controlla la congruità della loro nomina, verifica che nel registro del trattamento siano riportati tra i soggetti che trattano dati e che siano specificati, nell'informativa fornita ai vati interessati, i trattamenti da loro effettuati[145].

## 2.5. *I diritti dell'interessato*

Il Regolamento (UE) 2016/679 prevede una tutela effettiva, pratica ed efficace dei diritti e delle libertà degli interessati, intesi come persone fisiche direttamente o indirettamente identificati o identificabili, i cui dati personali sono oggetto del trattamento.

I diritti dell'interessato vengono disciplinati dall'art. 15 all'art. 22 del GDPR e costituiscono un corollario dei principi del trattamento.

Infatti, il principio di liceità e trasparenza sarebbe privo di contenuto se non fosse riconosciuto all'interessato il diritto di accedere ai dati e alle informazioni che lo riguardano; mentre, il principio di esattezza si esplica attraverso il diritto alla cancellazione, alla rettifica e all'aggiornamento dei dati personali.

[145] cfr. S. BONGIOVANNI, C. MOTTINO e M. PEREGO, *Formulario del DPO. Norme, giurisprudenza, strumenti operativi e modelli di atti*, I ed., G. Giappichelli Editore, Torino, 2021.

### 2.5.1. *Diritto di accesso*

L'art. 15, paragrafo 1 del GDPR statuisce che: «*L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni: a) le finalità del trattamento; b) le categorie di dati personali in questione; c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali; d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento; f) il diritto di proporre reclamo a un'autorità di controllo; g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine; h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato*».

Tale articolo statuisce una serie di obblighi in capo al titolare che prevedono di fornire all'interessato tutte le informazioni richieste, entro un termine ragionevole, e di ricorrere a tecnologie che danno la possibilità all'interessato di consultare direttamente i propri dati personali, purché non vi sia la lesione di diritti e libertà altrui[146]. Perciò, l'interessato ha diritto ad ottenere una copia dei dati trattati, anche in formato digitale, gratuitamente; nel caso richieda più copie gli potrà essere addebitato il relativo costo di estrazione e processazione[147].

[146] *Ex* Considerando n. 63 del GDPR.
[147] *Ex* art. 15, par. 3 del GDPR.

### 2.5.2. *Diritto limitazione e di rettifica del trattamento*

Il diritto alla limitazione, previsto all'art. 18 del GDPR, specifica il principio di limitazione della conservazione dei dati. Secondo tale articolo l'interessato ha diritto ad ottenere dal titolare del trattamento la limitazione del trattamento, quando ricorre una delle ipotesi previste; riassumendole tali ipotesi sono: contestazione dell'esattezza dei dati personali da parte dell'interessato; trattamento illecito per cui l'interessato si oppone alla cancellazione e chiede la limitazione dell'utilizzo; dati personali necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, benché il titolare non ne abbia più bisogno; infine, opposizione dell'interessato ai sensi dell'art. 21, paragrafo 1 del GDPR[148] e attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento.

I dati oggetto di limitazione potranno essere trattati solo previo consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, o per tutelare i diritti di un'altra persona fisica o giuridica, oppure per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

Qualora venga revocata la limitazione, l'interessato ha diritto ad essere informato sul trattamento che verrà effettuato in futuro.

Il diritto di rettifica è disciplinato all'art. 16 del GDPR e si riconnette al principio di esattezza e aggiornamento dei dati, per cui: «*L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa*».

[148] *Ex* art. 21, par. 1 del GDPR: «*L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria*».

### 2.5.3. *Diritto all'oblio*

Il diritto all'oblio viene disciplinato analiticamente all'art. 17 del GDPR e si può definire come il diritto alla cancellazione dei propri dati personali. Si riconosce all'interessato il diritto di chiedere che i propri dati personali siano cancellati e non più sottoposti al trattamento, in una serie di ipotesi: «[…] *a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento; c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2; d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1*».

Il titolare del trattamento, se ricorre uno delle ipotesi appena menzionate, è obbligato a provvedere alla cancellazione, senza ingiustificato ritardo. Inoltre, se ha reso pubblici i dati personali, tenendo conto della tecnologia disponibile e dei costi di attuazione, deve adottare le misure ragionevoli, anche tecniche, per informare i titolari del trattamento, che stanno trattando i dati personali, della richiesta mossa dall'interessato di cancellazione di qualsiasi *link*, copia o riproduzione dei suoi dati personali[149].

Posta tale regola il paragrafo 3 dell'art. 17 del GDPR pone un'eccezione, in un'ottica di bilanciamento di interessi contrapposti, esclude l'applicazione delle disposizioni prima dette qualora il trattamento sia necessario: «*a) per l'esercizio del diritto alla libertà di espressione e di informazione; b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è*

[149] *Ex* art. 17, paragrafo 2 del GDPR.

*soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento; c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3; d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria*».

Importante ricordare la sentenza nodale della Corte di Giustizia dell'Unione Europea che sancì il diritto all'oblio, si tratta della sentenza n. 317 del 13 maggio 2014 riguardante la causa C-131/12 *Google Spain SL, Google Inc.* contro *Agencia Española de Protecciòn de Datos (AEPD)*, *Mario Costeja González*[150]. Tale sentenza stabilì che nel

[150] In breve, il fatto: nel 2010 il sig. *Mario Costeja González*, cittadino spagnolo, ha presentato all' *Agencia Española de Protecciòn de Datos*, anche detta "AEPD", un reclamo contro La *Vanguardia Ediciones SL* (editore di un quotidiano largamente diffuso in Spagna), nonché contro *Google Spain* e *Google Inc.* Il sig. *Costeja González* faceva valere che, allorché il proprio nome veniva introdotto nel motore di ricerca *Google Search*, l'elenco di risultati mostrava dei *link* verso due pagine del quotidiano di *La Vanguardia*, datate gennaio e marzo 1998. Tali pagine annunciavano una vendita all'asta di immobili organizzata a seguito di un pignoramento effettuato per la riscossione coattiva di crediti previdenziali nei confronti del sig. *Costeja González*. Mediante detto reclamo, il sig. *Costeja González* chiedeva, da un lato, che fosse ordinato a La Vanguardia di sopprimere o modificare le pagine suddette (affinché i suoi dati personali non vi comparissero più) oppure di ricorrere a taluni strumenti forniti dai motori di ricerca per proteggere tali dati. Dall'altro lato, chiedeva che fosse ordinato a *Google Spain* o a *Google Inc.* di eliminare o di occultare i suoi dati personali, in modo che cessassero di comparire tra i risultati di ricerca e non figurassero più nei *link* di *La Vanguardia*. Il sig. *Costeja González* affermava in tale contesto che il pignoramento effettuato nei suoi confronti era stato interamente definito da svariati anni e che la menzione dello stesso era ormai priva di qualsiasi rilevanza. L'AEPD ha respinto il reclamo diretto contro *La Vanguardia*, ritenendo che l'editore avesse legittimamente pubblicato le informazioni in questione. Per contro, il reclamo è stato accolto nei confronti di *Google Spain* e *Google Inc.* L'AEPD ha chiesto a queste due società di adottare le misure necessarie per rimuovere i dati dai loro indici e per rendere impossibile in futuro l'accesso ai dati stessi. *Google Spain* e *Google Inc*. hanno proposto due ricorsi dinanzi all'*Audiencia Nacional,* chiedendo l'annullamento della decisione dell'AEPD. È in tale contesto che il giudice spagnolo ha sottoposto una serie di questioni alla Corte di giustizia. (cit. Corte di giustizia dell'Unione europea, comunicato stampa, n. 70/14 Lussemburgo, 13 maggio 2014, in *curia.europa.eu*). I quesiti posti alla Corte possono essere ricondotti in 4 gruppi, riguardanti: 1. l'ambito territoriale di applicazione della direttiva; 2. l'attività dei motori della ricerca quali fornitori di contenuti ossia, *in primis*, se essa possa essere riconducibile alla nozione di 'trattamento di dati' *ex* art. 2, lett. b) della direttiva e, in secondo luogo, se la società di gestione di tali motori possa ritenersi un "responsabile del trattamento" *ex* art. 2, lett. d) della medesima direttiva; 3. i "poteri" dell'AEPD, ossia se possa ordinare al *provider* di rimuovere le informazioni pubblicate da terzi, e rimanenti nella *web page* di origine, a prescindere sia dalla natura (lecita

caso in cui, a seguito di una ricerca effettuata a partire dal nome di una persona, l'elenco di risultati mostri *link* verso pagine *web* che contengono informazioni sulla persona in questione, questa può rivolgersi direttamente al gestore oppure, qualora questi non dia seguito alla sua domanda, adire le autorità competenti, per ottenere, in presenza di determinate condizioni, la soppressione di tale *link* dall'elenco di risultati[151]. Quindi, l'autorità di controllo o l'autorità giudiziaria, all'esito della valutazione dei presupposti di applicazione degli artt. 12, lett. b), e 14, co. 1, lett. a), Dir. 95/46, possono ordinare al gestore del servizio di cancellare, dall'elenco di risultati che appare a seguito di una ricerca, i *link* verso pagine *web* pubblicate da terzi (nel caso di specie in una testata giornalistica *online*) e contenenti informazioni relative a una persona. Il fornitore del servizio è obbligato, inoltre, a sopprimere gli stessi *link* anche nel caso in cui il nome o le informazioni non vengano previamente o simultaneamente cancellati dalle pagine *web* del quotidiano, eventualmente quando la loro pubblicazione sia altresì di per sé lecita[152].

A fondamento del diritto all'oblio vi è il principio secondo cui il trattamento dei dati inizialmente lecito potrebbe divenire con il tempo illecito rispetto al Regolamento, questo qualora i dati non siano più necessari, perciò risultino essere inadeguati, non più pertinenti ovvero eccessivi.

Inoltre, si può notare che, secondo la Corte, i diritti fondamentali di cui agli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione Europea[153] prevalgono, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse del pubblico degli utenti a trovare l'informazione in occasione di una ricerca *online* relativa ad una persona determinata; ferme restando le eccezioni legate, ad esempio, al ruolo ricoperto da tale persona nella vita pubblica, che potrebbe giustificare la prevalenza dell'interesse degli utenti ad avere accesso all'informazione.

---

o illecita) della pubblicazione, sia dall'autorizzazione del titolare della pagina *web* in cui essa è inserita; 4. la portata del diritto di cancellazione e di opposizione al trattamento dei dati in rapporto al c.d. diritto all'oblio e alla libertà di espressione (cit. R. FLOR, *Dalla data retention al diritto all'oblio*, 2014, p. 228).

[151] cit. Corte di giustizia dell'Unione europea, comunicato stampa n. 70/14, Lussemburgo, 13 maggio 2014, in *curia.europa.eu*.

[152] cit. A. CADOPPI [et. al.], op. cit., p. 128.

[153] L'art. 7 della Carta dei diritti fondamentali dell'Unione si riferisce al "rispetto della vita privata e della vita familiare" e l'art. 8 alla "protezione dei dati di carattere personale".

### 2.5.4. *Diritto alla portabilità dei dati*

Il diritto alla portabilità dei dati costituisce una delle novità più rilevanti, sia perché trova la sua logica nel progresso tecnologico che caratterizza l'era digitale, invero, tale diritto è attivabile solo con riguardo ai dati conservati su supporti automatizzati; sia perché rende necessario prevedere ulteriori strumenti che consentano all'interessato di rafforzare il controllo sui propri dati.

Viene disciplinato all'art. 20 del GDPR il quale stabilisce che l'interessato ha diritto di ricevere, in un formato strutturato, di uso comune e leggibile da un dispositivo automatico, i dati personali che lo riguardano e ha diritto di trasmettere tali dati ad un altro titolare, senza impedimenti qualora il trattamento si basi sul consenso e sia effettuato con mezzi automatizzati.

L'interessato, in pratica, può svolgere tre attività: ricevere i dati dal titolare che li ha trattati, trasmetterli ad un diverso titolare ovvero chiedere che questa operazione sia compiuta direttamente tra titolari. Dette attività sono realizzabili nel caso in cui i dati personali vengano conservati in un formato strutturato, di uso comune e leggibile da un dispositivo automatico[154].

### 2.5.5. *Diritto di opposizione*

Il diritto di opposizione prevede che l'interessato possa opporsi al trattamento dei propri dati e all'eventuale profilazione connessa; di conseguenza, il titolare è obbligato ad astenersi dal trattamento, a meno che non sussistano cause di forza maggiore tali da prevalere su suddetto diritto, oppure il trattamento sia necessario all'accertamento,

[154] Per esempio, uno strumento utilizzabile per rendere effettivo tale diritto sono i fogli *Excel*. Mentre, un PDF scansionato, benché suscettibile di essere "leggibile" da parte dell'interessato, non presenta la caratteristica dell'interoperabilità tra dispositivi elettronici automatici, e quindi risulta insuscettibile di rispondere ai requisiti dell'art. 20 del GDPR (cit. M. MARTORANA, A. TESORO, A. BARBERISI (a cura di), op. cit., p. 49).

all'esercizio o alla difesa di un diritto in sede giudiziaria, o ancora, il trattamento sia necessario all'esecuzione di un compito di interesse pubblico.

Tale diritto è previsto all'art. 21 del GDPR[155], in virtù del principio di contemperamento di interessi contrapposti.

Nel Considerando n. 69 si specifica che: «*È opportuno che incomba al titolare del trattamento dimostrare che i suoi interessi legittimi cogenti prevalgono sugli interessi o sui diritti e sulle libertà fondamentali dell'interessato*». Dunque, oltre all'obbligo di cessazione del trattamento, sorge in capo al titolare anche il dovere di dimostrare la legittimità e la necessità del trattamento in caso egli ritenga di doverlo continuare.

### 2.5.6. *Diritto di revocare il consenso*

L'art. 7, paragrafo 3 del GDPR statuisce che: «*L'interessato ha diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il*

[155] *Ex* art. 21 del GDPR: «*1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. 2. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto. 3. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità. 4. Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato. 5. Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche. 6. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico*».

*proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato*».

Tale diritto è un corollario del principio di libertà del consenso, per cui il consenso è libero solo se liberamente revocabile.

Il consenso funge da base giuridica del trattamento, qualora questo venga meno il titolare dovrà cessare il trattamento e procedere alla cancellazione dei dati personali.

Per quanto riguarda la modalità di revoca del consenso il Regolamento statuisce in un'ottica di semplificazione delle procedure, che dovrà avvenire con la stessa facilità con cui il consenso è stato accordato[156].

### 2.6. *La violazione o la perdita dei dati*

Si utilizza il termine "*data breach*" per indicare un incidente di sicurezza che cagiona una violazione tale da comportare, in modo accidentale e/o illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, che compromette la riservatezza, l'integrità o la disponibilità di dati personali[157].

L'incidente di sicurezza si verifica qualora vi sia un'intrusione nei sistemi aziendali, per cui i dati personali di un soggetto, protetti e riservati, entrano in possesso, anche provvisoriamente, di un soggetto non autorizzato; ne consegue una divulgazione di tali dati, che dovrebbero rimanere riservati e confidenziali, in un ambiente privo di misure di sicurezza.

Il *data breach* si può verificare, per esempio, nel caso di: perdita accidentale, furto, infedeltà aziendale ed accesso abusivo.

---

[156] Per esempio, se per ricevere la *newsletter* di un'azienda, contenente campagne pubblicitarie, è stato sufficiente inserire la propria *e-mail* e cliccare su "accetta", sarà inammissibile essere costretti, per revocare il consenso, alla stampa di un modulo cartaceo da compilare e inviare alla sede legale dell'azienda a mezzo di raccomandata con ricevuta di ritorno, ben potendo, il consenso, essere revocato tramite una richiesta telematica attraverso un semplice "*click*" (cit. M. MARTORANA, A. TESORO, A. BARBERISI (a cura di), op. cit., p. 49).

[157] *Ex* art. 4, par. 1 del GDPR.

In questi casi ciò che rileva è la situazione che si viene a creare, caratterizzata da un grave pregiudizio per i diritti e le libertà degli interessati; pregiudizio che dev'essere necessariamente fronteggiato, adeguatamente e tempestivamente, altrimenti potrebbe comportare un danno fisico, materiale o immateriale, sociale o addirittura economico alla persona fisica interessata.

Il Regolamento prevede una serie di specifiche procedure da seguire all'art. 33, secondo le quali il titolare del trattamento, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui viene a conoscenza della violazione, la deve notificare al Garante per la protezione dei dati personali, a meno che sia improbabile che la violazione comporti un rischio per i diritti e le libertà delle persone fisiche.

Qualora la violazione sia avvenuta presso il responsabile del trattamento, questo sarà tenuto ad informare tempestivamente il titolare in modo tale che quest'ultimo possa attivarsi come appena detto.

L'obbiettivo della notifica è di consentire al Garante della *privacy* di potersi attivare, il prima possibile, e valutare la gravità della situazione per poter stabilire le misure correttive da imporre al titolare, dimodoché si riducano al minimo i pericoli.

Inoltre, qualora il rischio di compromissione dei diritti risulti essere elevato dovranno essere tempestivamente informati anche i diretti interessati, sulla base di un ordine dell'autorità di vigilanza diretto al titolare dopo aver svolto una valutazione dei rischi; i titolari comunicano agli interessati le informazioni concernenti i rischi che si sono presentati e i passaggi che si possono adottare per proteggersi[158].

È necessario che i titolari del trattamento pianifichino in anticipo e mettano in atto

---

[158] *Ex* Considerando n. 86 del GDPR: «*Il titolare del trattamento dovrebbe comunicare all' interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie. La comunicazione dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione*».

procedure volte a rilevare e contenere prontamente le violazioni, affinché si possa prevenire efficacemente la perdita di dati.

L'art. 32 del GDPR, rubricato "sicurezza del trattamento" sancisce che dovrebbero essere considerati: «*la capacità di garantire la riservatezza in corso, integrità, disponibilità e resilienza dei sistemi e dei servizi di elaborazione e la capacità di ripristinare la disponibilità e l'accesso ai dati personali in modo tempestivo in caso di incidente fisico o tecnico*», affinché siano attuate le misure tecniche ed organizzative atte a garantire un livello di sicurezza adeguato al rischio.

Non si tratta di un obbligo generale, il titolare del trattamento dovrà valutare, caso per caso, la probabilità e la gravità dell'impatto sui diritti e le libertà delle persone fisiche.

La mancata segnalazione, attraverso la notifica al Garante, può comportare una sanzione al titolare del trattamento.

Per quanto attiene al contenuto della notifica, l'art. 33, paragrafo 2 del GDPR prevede che sia, quanto più possibile, completa, deve contenere informazioni circa la natura della violazione, i contatti del responsabile o di chiunque sia incaricato a dare informazioni in merito, una valutazione sulle probabili conseguenze e la descrizione delle misure adottate ovvero di quelle che si intendono adottare per porre rimedio al *data breach* o almeno per limitarne gli effetti negativi.

L'Autorità garante ha messo a disposizione un *facsimile* di comunicazione[159], nel quale si richiede di indicare: quando si è verificata la violazione; se la violazione è avvenuta prima delle 72 ore dalla compilazione della notifica si richiede di indicare le ragioni che hanno ostacolato un'immediata rilevazione dell'evento; dov'è avvenuta la violazione; una breve descrizione della tipologia di violazione; il dispositivo oggetto della violazione; la descrizione dei sistemi di elaborazione o memorizzazione dei dati coinvolti; quante persone sono state colpite; che tipo di dati sono oggetto di violazione; il livello di gravità; infine, le misure tecniche e organizzative applicate ai dati oggetto di violazione.

[159] Consultabile sul sito *servizi.gpdp.it*, nel quale, inoltre, viene predisposto il procedimento telematico per inviare la notifica.

## 2.7. *Ricorsi e sanzioni*

L'interessato, qualora ritenga che il trattamento che lo riguardi violi il Regolamento ha il diritto di proporre reclamo ad un'autorità di controllo, segnatamente dello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione[160]. Se poi l'interessato non è soddisfatto della decisione presa dall'autorità di controllo o se questa manca di riferirgli circa lo stato o l'esito del reclamo entro tre mesi, può proporre un ricorso giurisdizionale effettivo.

Il ricorso può essere presentato anche contro il titolare o il responsabile del trattamento, quando si ritiene che questi abbiano violato le disposizioni del Regolamento, a condizione che venga presentato alle autorità dello Stato in cui sono stabiliti o in cui l'interessato risiede abitualmente[161].

Il GDPR ammette che l'interessato si possa far rappresentare da un'organizzazione o un'associazione senza scopo di lucro, a patto che lo scopo statutario di questo organo riguardi la difesa dei diritti e delle libertà concernenti la *privacy*[162].

In un'ottica globale, nel caso in cui siano in corso azioni legali contro lo stesso soggetto in vari Stati membri, le autorità giudiziarie, venute a conoscenza dell'esistenza di un procedimento pendente contro lo stesso soggetto in un altro Stato, possano sospendere le proprie azioni.

Ai sensi dell'art. 82 del GDPR se l'interessato ha subito un danno materiale o immateriale causato dalla violazione delle disposizioni, ha diritto ad ottenere il risarcimento del danno da parte del titolare o del responsabile del trattamento, salva la possibilità di quest'ultimi di dimostrare che la violazione non è loro imputabile in alcun modo. Inoltre, il medesimo articolo al paragrafo 4 prevede la responsabilità solidale per l'intero ammontare del danno, da dividere fra tutti i responsabili e i titolari coinvolti.

Una delle importanti innovazioni apportate dal Regolamento (UE) 2016/679

[160] *Ex* art. 77 del GDPR.
[161] *Ex* art. 79 del GDPR.
[162] *Ex* art. 80 del GDPR.

riguarda le sanzioni da applicare in caso di violazione delle disposizioni in esso contenute. La previgente Direttiva 95/46/CE si limitava ad imporre una generica previsione di sanzioni, rimandando agli Stati membri la puntuale definizione della materia; mentre, il GDPR prevede una disciplina puntuale ed analitica delle sanzioni.

La disciplina dell'apparato sanzionatorio è contenuta, principalmente, nell'art. 83 del GDPR nel quale vengono previsti una serie di casi in cui dev'essere irrogata la sanzione amministrativa pecuniaria e si stabilisce il suo importo massimo.

Il paragrafo 4 dell'art. 83 del GDPR stabilisce che le sanzioni amministrative pecuniarie hanno un importo massimo di 10.000.000 euro, o per le imprese fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, nei seguenti casi: violazione degli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43[163]; gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43; e gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4.

Il paragrafo 5 dell'art. 83 del GDPR stabilisce che le sanzioni amministrative pecuniarie hanno importo massimo di 20.000.000 euro, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, nei seguenti casi: violazione dei principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9; violazione dei diritti degli interessati a norma degli articoli da 12 a 22; violazione dei trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49; violazione di un qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX[164].; inosservanza di un ordine, di una limitazione provvisoria o

[163] Riassumendo, detti articoli si riferiscono: violazione della disciplina sul consenso con riferimento ai minori; trattamento che non richiede l'identificazione; violazione della *privacy by design* e *privacy by default*; violazione della disciplina sulla contitolarità del trattamento; violazione della disciplina sulla designazione del rappresentante; violazione della disciplina sul trattamento sotto l'autorità del titolare del trattamento o del responsabile; erronea tenuta dei registri; mancata cooperazione con le autorità; mancata adozione di misure di sicurezza; mancata o irregolare notifica di una violazione all'autorità; violazione della disciplina del *data breach*; violazione della disciplina dalla valutazione d'impatto; violazioni inerenti al *Data Protection Officer*; violazioni in materia di certificazioni da parte del titolare o del responsabile del trattamento.

[164] Riassumendo, detti articoli si riferiscono: violazione dei principi di base del trattamento;

definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

Infine, il paragrafo 6 dell'art. 83 del GDPR prevede l'applicazione del secondo regime sanzionatorio, del paragrafo 5, anche in caso di inosservanza di un ordine da parte dell'autorità di controllo.

Per quanto concerne le sanzioni penali, secondo quanto stabilito dall'art. 84, paragrafo 1 del GDPR, il quale parla in generale di "altre sanzioni", queste devono essere stabilite dalle norme degli Stati membri, purché siano effettive, proporzionate e dissuasive. A tal proposito merita ricordare gli artt. da 167 a 171 del D. Lgs. n. 169/2003, sul trattamento illecito dei dati, sulle falsità nelle dichiarazioni e notificazioni del Garante, sull'omessa adozione di misure di sicurezza, sull'inosservanza di un provvedimento del Garante e sulla violazione del trattamento dei dati derivati da violazione degli artt. 4 e 8, Legge 20 maggio 1970, n. 300[165].

Fondamentale in tema di sanzioni è il ruolo ricoperto dall'Autorità garante. L'art. 83, paragrafo 1 del GDPR stabilisce che: «*Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive*». Per autorità di controllo si intende, secondo quanto detto all'art. 4, paragrafo 1, n. 21) del GDPR: «*l'autorità pubblica indipendente istituita da uno Stato membro*».

In Italia l'autorità di controllo è il Garante per la protezione dei dati personali, anche detto Garante della *privacy* o GPDP[166]. Le caratteristiche base del Garante si possono riassumere in indipendenza e competenza. Non possono farsi influenzare da

violazione dei diritti dell'interessato; violazione della normativa sul trasferimento transfrontaliero dei dati personali; violazione di qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate, in materia di libertà d'espressione e informazione, documenti ufficiali, numero di identificazione nazionale, rapporti di lavoro, archiviazione nel pubblico interesse, ricerca scientifica o storica o a fini statistici, segretezza, chiese e associazioni religiose.

[165] La Legge 20 maggio 1970, n. 300 reca le norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento.

[166] Il Garante della *privacy* si può definire come un'autorità amministrativa indipendente italiana,

pressioni esterne, non accettano istruzioni da alcuno, si astengono da qualunque azione incompatibile con le loro funzioni e ogni suo membro possiede le qualifiche, l'esperienza e le competenze richieste per espletare i compiti assegnati.

I compiti e i poteri affidati al Garante sono previsti nel dettaglio agli artt. 57 e 58 del GDPR, tra i quali si riconosce un potere di indagine per riuscire tempestivamente ad individuare eventuali irregolarità e violazioni; altrettanto importante, lo *ius corrigendi* che ha a disposizione qualora le violazioni e le irregolarità si siano già verificate.

In materia di sanzioni rileva il potere del Garante previsto all'art. 58, paragrafo 2, lett. i) del GDPR per cui può: «*infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle misure di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso*». Perciò, tenendo conto anche delle Linee guida del Garante della *privacy* emanate il 10 ottobre 2017, questa autorità qualora debba infliggere una sanzione deve seguire i seguenti parametri: imporre sanzioni equivalenti alla violazione; le sanzioni amministrative pecuniarie dovrebbero essere effettive, proporzionate e dissuasive; deve effettuare una valutazione in ogni singolo caso. Ancora, l'art. 83, paragrafo 2 del GDPR[167] stabilisce altri parametri che da seguire al momento della valutazione della violazione.

---

istituita dalla Legge n. 675 del 31 dicembre 1996, che ha il compito di assicurare la tutela dei diritti e delle libertà fondamentali e il rispetto della dignità nel trattamento dei dati personali.

[167] *Ex* art. 83, par. 2 del GDPR: «*Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi: a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito; b) il carattere doloso o colposo della violazione; c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati; d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32; e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento; f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi; g) le categorie di dati personali interessate dalla violazione; h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione; i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti; j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e k) eventuali altri fattori aggravanti o attenuanti*

Per capire l'impatto che tale sistema sanzionatorio può avere nei confronti delle aziende basta visionare qualche caso recente di violazione del Regolamento. Per esempio, nel 2022 la sanzione più alta è stata inflitta a "*Meta Platforms, Inc.*"[168] dalla Commissione irlandese per la protezione dei dati. Detta sanzione ammontava a 405 milioni di euro, per la violazione della *privacy* dei minori da parte di *Instagram* attraverso la pubblicazione di indirizzi *e-mail* e numeri di telefono. La piattaforma consentiva a ragazzi di età compresa tra i 13 ei 17 anni di utilizzare account aziendali in cui era possibile accedere sia agli indirizzi *e-mail* che ai numeri di telefono; inoltre, gli *account* non erano privati per impostazione predefinita e in alcuni casi potevano essere visualizzati dal pubblico[169].

## 2.8. *Il trasferimento dei dati verso Paesi terzi o organizzazioni internazionali*

Una delle possibili definizioni di "trasferimento di dati personali" è: «*Tutti i casi in cui un titolare del trattamento si attiva per rendere disponibili dati personali ad un soggetto terzo, che si trova in un Paese terzo*»[170].

La necessità, per un titolare del trattamento, di trasferire i dati da un Paese ad un altro tramite un'operazione di comunicazione è un fatto del tutto normale e particolarmente diffuso.

In questo caso non è sufficiente informare l'interessato, affinché il trasferimento sia legittimo, perché in aggiunta si richiede che il soggetto estero garantisca un livello di sicurezza equivalente a quello europeo.

Il Capo V del Regolamento (UE) 2016/679 disciplina il trasferimento di dati

---

*applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione*».

[168] *Meta Platforms, Inc.* è un'impresa statunitense che controlla i servizi di rete come *Facebook* e *Instagram*, i servizi di messaggistica istantanea come *Whatsapp* e *Messanger* e sviluppa visori di realtà virtuale. È stata fondata nel 2004 da Mark Zuckerberg, Eduardo Saverin, Andrew McCollum, Dustin Moskovitz e Chris Hughes.

[169] cit. *Privacy dei minori violata su Instagram, 450 mln di multa a Meta*, in *privacy.it*, 2022.

[170] cit. A. BIASIOTTI, *Il nuovo regolamento europeo sulla protezione dei dati*, III ed., Roma, 2018, p. 774.

personali verso Paesi terzi od organizzazioni internazionali, secondo l'art. 44 il principio generale da rispettare è: «*Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato*».

Benché i Paesi *extra* UE non siano direttamente soggetti alle disposizioni del Regolamento, quest'ultimo si applica: «*Al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione*», così come disposto dall'art. 3, paragrafo 1 del GDPR.

L'art. 45 del GDPR dispone che il trasferimento sia ammesso se la Commissione europea ha deciso che il Paese terzo, un territorio o uno o più settori specifici al suo interno, o l'organizzazione internazionale in questione, garantiscano un livello di protezione adeguato; in tal caso, non è necessaria un'autorizzazione specifica. Tale livello è adeguato di protezione se garantisce la certezza del diritto e l'uniformità in tutta l'Unione[171].

L'Art. 46 del GDPR stabilisce che, in mancanza di una decisione ai sensi dell'art. 45, il titolare del trattamento può trasferire i dati personali verso un Paese terzo od un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.

Infine, l'art. 47, paragrafo 2 del GDPR[172] sancisce una serie di norme vincolanti

[171] *Ex* Considerando n. 103 del GDPR.
[172] *Ex* art. 47, par. 2 del GDPR: «*2. Le norme vincolanti d'impresa di cui al paragrafo 1 specificano*

per l'impresa, le quali costituiscono uno strumento, predisposto dal legislatore europeo, per far fronte alla necessità di trasferire dati tra imprese appartenenti allo stesso gruppo multinazionale, qualora talune delle stesse siano stabilite su un territorio *extra* UE. Si tratta di una serie di clausole contrattuali che fissano dei principi comuni in materia di protezione dei dati personali che le aziende, appartenenti al gruppo, devono rispettare.

---

*almeno: a) la struttura e le coordinate di contatto del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e di ciascuno dei suoi membri; b) i trasferimenti o il complesso di trasferimenti di dati, in particolare le categorie di dati personali, il tipo di trattamento e relative finalità, il tipo di interessati cui si riferiscono i dati e l'identificazione del paese terzo o dei paesi terzi in questione; c) la loro natura giuridicamente vincolante, a livello sia interno che esterno; d) l'applicazione dei principi generali di protezione dei dati, in particolare in relazione alla limitazione della finalità, alla minimizzazione dei dati, alla limitazione del periodo di conservazione, alla qualità dei dati, alla protezione fin dalla progettazione e alla protezione per impostazione predefinita, alla base giuridica del trattamento e al trattamento di categorie particolari di dati personali, le misure a garanzia della sicurezza dei dati e i requisiti per i trasferimenti successivi ad organismi che non sono vincolati dalle norme vincolanti d'impresa; e) i diritti dell'interessato in relazione al trattamento e i mezzi per esercitarli, compresi il diritto di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione ai sensi dell'articolo 22, il diritto di proporre reclamo all'autorità di controllo competente e di ricorrere alle autorità giurisdizionali competenti degli Stati membri conformemente all'articolo 79, e il diritto di ottenere riparazione e, se del caso, il risarcimento per violazione delle norme vincolanti d'impresa; f) il fatto che il titolare del trattamento o il responsabile del trattamento stabilito nel territorio di uno Stato membro si assume la responsabilità per qualunque violazione delle norme vincolanti d'impresa commesse da un membro interessato non stabilito nell'Unione; il titolare del trattamento o il responsabile del* trattamento *può essere esonerato in tutto o in parte da tale responsabilità solo se dimostra che l'evento dannoso non è imputabile al membro in questione; g) le modalità in base alle quali sono fornite all'interessato le informazioni sulle norme vincolanti d'impresa, in particolare sulle disposizioni di cui alle lettere d), e) e f), in aggiunta alle informazioni di cui agli articoli 13 e 14; h) i compiti di qualunque responsabile della protezione dei dati designato ai sensi dell'articolo 37 o di ogni altra persona o entità incaricata del controllo del rispetto delle norme vincolanti d'impresa all'interno del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e il controllo della formazione e della gestione dei reclami; ([1]) i) le procedure di reclamo; j) i meccanismi all'interno del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune per garantire la verifica della conformità alle norme vincolanti d'impresa. Tali meccanismi comprendono verifiche sulla protezione dei dati e metodi per assicurare provvedimenti correttivi intesi a proteggere i diritti dell'interessato. I risultati di tale verifica dovrebbero essere comunicati alla persona o entità di cui alla lettera h) e all'organo amministrativo dell'impresa controllante del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e dovrebbero essere disponibili su richiesta all'autorità di controllo competente; k) i meccanismi per riferire e registrare le modifiche delle norme e comunicarle all'autorità di controllo; l) il meccanismo di cooperazione con l'autorità di controllo per garantire la conformità da parte di ogni membro del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune, in particolare la messa a disposizione dell'autorità di controllo dei risultati delle verifiche delle misure di cui alla lettera j); m) i meccanismi per segnalare all'autorità di controllo competente ogni requisito di legge cui è soggetto un membro del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune in un paese terzo che potrebbe avere effetti negativi sostanziali sulle garanzie fornite dalle norme vincolanti d'impresa; e n) l'appropriata formazione in materia di protezione dei dati al personale che ha accesso permanente o regolare ai dati personali*».

# CAPITOLO III

# LA RESPONSABILITÀ AMMINISTRATIVA DA REATO DELL'ENTE

# AI SENSI DEL D. LGS. 231/2001

SOMMARIO: 3.1. Dal principio *societas delinquere non potest* alla responsabilità amministrativa da reato dell'ente. – 3.2. I requisiti e presupposti della responsabilità amministrativa da reato dell'ente. – 3.2.1. I soggetti destinatari della disciplina. – 3.2.2. Le nozioni di "interesse" e "vantaggio". – 3.2.3. I reati presupposto. – 3.2.4. La colpa per organizzazione. – 3.2.5. Art. 6 e art. 7 del D. Lgs. 231/2001. – 3.2.6. Il principio di autonomia. – 3.2.7. La delega di funzioni. – 3.2.8. Il sistema sanzionatorio. – 3.3. Profili di responsabilità degli enti nei reati informatici e nel trattamento illecito di dati *ex* art. 24-*bis* D. Lgs. 231/2001. – 3.3.1. Il trattamento illecito di dati *ex* art. 167 del Codice della *privacy*. – 3.3.2. Conclusioni. – 3.4. Clausole di esonero della responsabilità dell'ente: i modelli organizzativi nel dettaglio. – 3.4.1. Il Modello 231. – 3.4.1.1. Il MOGC idoneo a prevenire la commissione di reati informatici. – 3.4.2. L'Organismo di Vigilanza.

## 3.1. *Dal principio* societas delinquere non potest *alla responsabilità amministrativa da reato dell'ente prevista dal D. Lgs. 231/2001*

Nel sistema penale italiano vige tradizionalmente il principio, di origine romanistica[173], *societas delinquere non potest* che affonda le proprie radici nella concezione personalistica della responsabilità penale[174], basata sul presupposto che la

[173] A tal proposito si ricordi il giurista romano Gaio, il quale negava la possibilità di perseguire gli enti; viceversa, il giurista romano Ulpiano sosteneva che l'accusa potesse aver luogo contro coloro che amministravano la città, e non contro la città (cfr. S. LONGHI, *La persona giuridica come soggetto di responsabilità penale*, in *Rivista penale*, Torino, 1906, p. 16).

[174] cfr. F. MANTOVANI, op. cit., pp. 22 ss.

pena, per la sua natura e per le sue funzioni, è considerata alla stregua di un trattamento sanzionatorio rivolto esclusivamente alla persona fisica.

Non vi è, all'interno della nostra legislazione penale, una norma che esplicitamente neghi la responsabilità penale delle persone giuridiche, perciò a tale conclusione si giunge analizzando i diversi principi base del diritto penale sostanziale.

Il rifiuto di riconoscere una responsabilità penale dell'ente[175] si ricollega ad una concezione psicologica e naturalistica della colpevolezza, intesa quale determinazione volitiva riprovevole dell'agente, connaturata, in quanto tale, alla sola persona fisica, essendo l'ente privo di psiche[176].

Il fondamento giuridico di detto principio si ritrova all'interno della Costituzione, l'art. 27 Cost. sancisce che: «*la responsabilità penale è personale*», per cui ammettere la responsabilità dell'ente, e dunque di un soggetto differente da quello che ha materialmente posto in essere la condotta costituente reato, contrasterebbe con il dettato costituzionale[177].

Si predilige la prospettiva secondo cui vi debba essere una necessaria corrispondenza tra il reo e il destinatario della sanzione; a tal proposito, corrispondere la pena ad un ente, intaccando il suo patrimonio, potrebbe colpire ingiustamente soggetti terzi estranei rispetto alla realizzazione dell'illecito.

Nel corso degli anni, con l'evolversi della società industriale, il dogma *societas*

---

[175] La denominazione di "ente" viene genericamente usata nelle leggi e nelle discipline giuridiche per indicare organismi e istituti caratterizzati dalla presenza di interessi e finalità più o meno superindividuali, la cui unificazione dà strutturalmente luogo alla creazione di organi e uffici funzionalmente rivolti alla realizzazione di un certo scopo tipico. È fenomeno squisitamente giuridico, risultato della creazione di un soggetto, in seguito alla quale un organismo non esistente sul piano naturalistico assume esistenza sul piano giuridico e si presenta dotato di capacità di agire per il perseguimento dei propri fini (cit. Enciclopedia online, in *treccani.it*).

[176] cfr. F. PALAZZO, *Corso di diritto penale, parte generale*, Torino, 2016, p. 53.

[177] A tal proposito si evidenziano due tesi della dottrina. Secondo una prima tesi, che interpreta la norma costituzionale in un'accezione più ristretta, si vuole soltanto vietare la responsabilità penale "per fatto altrui", la società non potrebbe rispondere penalmente per la condotta (altrui) di un suo organo. Mentre, secondo un'interpretazione più ampia, si identifica il carattere personale della responsabilità penale con la responsabilità ancorata al "principio di colpevolezza", la società non potrebbe rispondere personalmente perché incapace di atteggiamento volitivo colpevole (cfr. G. FIANDACA, E. MUSCO, *Diritto penale, parte generale*, VIII ed., Zanichelli, Bologna, 2023, p. 177).

*delinquere non potest* è entrato in crisi. Tra i più gravi episodi criminosi, lesivi di interessi collettivi, vi sono vere e proprie manifestazioni di criminalità d'impresa o anche detta societaria; si tratta di fenomeni già da tempo conosciuti, ma che solo recentemente hanno assunto un rilievo importante, generando patologie anche a livello internazionale.

La svolta si è verificata grazie a spinte sovranazionali e comparatistiche[178], una serie di normative comunitarie[179] ed internazionali hanno imposto ai singoli Stati membri di introdurre siffatta forma di responsabilità. Da ricordare anche l'intento di allineare il mondo continentale all'impostazione del mondo anglosassone, che da ormai decenni era giunto a configurare la responsabilità penale nei confronti delle persone giuridiche[180].

Il problema sorge in tutti quei casi in cui l'illecito costituisce la conseguenza di scelte inerenti alla politica d'impresa, per cui la mancata punizione dell'impresa si traduce in un ingiustificato accollo di responsabilità di un altro soggetto, che sembrerebbe assumere il ruolo di capro espiatorio. Vi sono diverse forme di criminalità nelle quali il soggetto attivo del reato è sostanzialmente l'ente.

Una volta preso atto dell'esigenza politico-criminale di predisporre sanzioni anche a carico di enti collettivi, ci si rende conto dell'inadeguatezza della concezione personalistica della pena e ci si trova in difficoltà nell' individuare concretamente i trattamenti sanzionatori da poter applicare.

Le effettive scelte decisionali si riconducono alla persona giuridica e il ruolo della persona fisica, che rappresenta l'ente, è spesso marginale. Anche qualora la persona fisica, parte dell'ente, possa essere considerata responsabile, la pena inflitta solo ad essa, avrebbe un'efficacia limitata poiché escluderebbe proprio il soggetto, ente giuridico, a cui è

---

[178] Tra le spinte comparatistiche, a livello esemplificativo troviamo: il codice penale francese del 1994 che ha accolto il principio della responsabilità penale delle *personnes morales*, così come il codice olandese del 1996 e quello finlandese, il danese e in parte il portoghese che contemplano la responsabilità penale dei soggetti collettivi (cfr. E. AMATI, *La responsabilità da reato degli enti,* UTET Giuridica, 2007, p. 8).

[179] Da ricordare la Raccomandazione del Comitato dei ministri del Consiglio d'Europa del 1998 con la quale si invitavano gli Stati membri a promuovere la adozione di misure (anche di natura penale) finalizzate a rendere le imprese responsabili per i reati commessi nell'esercizio delle loro attività, indipendentemente dai regimi di responsabilità civile in vigore.

[180] Nel mondo anglosassone si utilizza il termine "*corporate crime*" per indicare i delitti commessi da un ente societario e per i quali si applica una sanzione penale.

effettivamente riconducibile la commissione del reato; in tal modo la pena non potrebbe assolvere alla sua funzione dissuasiva, in senso generalpreventivo[181], nei confronti del soggetto quale centro operativo della criminalità d'impresa.

Si fa leva sulla teoria c.d. organicistica della persona giuridica[182], secondo la quale all'ente collettivo, in virtù di un rapporto di rappresentanza organica tra di esso e le persone fisiche che lo compongono e ne determinano la volontà e l'azione, si riconosce una soggettività reale, per cui l'attività compiuta dagli organi può essere ad esso direttamente imputata[183].

Per superare un altro importante ostacolo interpretativo, ovvero se l'ente collettivo può agire con dolo o con colpa, si propone di configurare contro la persona giuridica sanzioni aventi il carattere di misure di sicurezza più che di pene in senso stretto; sul presupposto che le misure di sicurezza si applicano qualora vi sia la pericolosità sociale e non la colpevolezza del destinatario. Tale soluzione non appare del tutto coerente, la condizione di pericolosità sociale non può prescindere da elementi psicologici, che difficilmente si riconoscono in un ente, ed inoltre è strettamente connessa alla risocializzazione, poco plausibile per un ente.

---

[181] Secondo la teoria generalpreventiva occorre partire dal dato di fatto incontrovertibile per cui la pena, prima di essere irrogata, viene minacciata. In questa fase lo scopo del legislatore non può che essere quello preventivo e dubitare di ciò, scrive F. Antolisei «*sarebbe come dubitare della stessa esistenza del sole*». Se questo è vero, però, allora ne discende come logica conseguenza che una pena minacciata, per essere veramente efficace, debba anche essere eseguita, a meno di non perdere il suo potere deterrente. La tesi della prevenzione generale ha quindi come conseguenza che la pena debba essere inflitta prontamente e in modo certo, a prezzo di vanificare lo stesso scopo per cui essa viene comminata. Altra conseguenza di rilievo è che la sanzione sarà tanto più efficace quanto più sarà elevata, il che può comportare anche l'inflizione delle cosiddette pene esemplari. È chiaro che la funzione preventiva è tantopiù efficace quanto più il diritto penale coincide con la morale corrente in una data società; perché tantopiù un comportamento vietato è sentito come immorale dagli individui e tantopiù questi saranno portati a seguirlo; al contrario tantopiù un comportamento vietato sarà considerato moralmente lecito, maggiore sarà la spinta che un soggetto sentirà nel violare la norma (cit. P. FRANCESCHETTI, *Pena*, in *AltalexPedia*, 2017).

[182] Ci si riferisce alla teoria organicistica dello Stato, la quale ha fatto si che l'apparato statuale apparisse come struttura superiore ed in grado di autodeterminare le proprie azioni mediante la volontà dei propri organi. In questo modo, all'ente giuridico non solo è imputabile l'effetto giuridico, ma anche l'atto che lo aveva prodotto (cit. P. LA SELVA, *La responsabilità amministrativa degli enti*, in *iusinitinere.it*, 2017).

[183] cfr. A. DE MARSICO, in *La difesa sociale*, il quale sostiene come non appaia corretto né conforme alla realtà escludere la responsabilità degli enti partendo dall'assunto che le società non possano compiere processi volitivi, si deve accettare che dall'unione indistinta di più soggettività individuali nasce e si riconosce una nuova soggettività (la società, per l'appunto), ed a tale nuova creazione non venga poi riconosciuta la possibilità di agire secondo una sua volontà, distinta ed autonoma rispetto a quella dei suoi creatori.

Il D. Lgs. 231/2001[184], attuativo della Legge delega 29 settembre 2000, n. 300[185], ha introdotto per la prima volta nell'ordinamento italiano l'istituto della responsabilità c.d. amministrativa degli enti e delle società per alcuni reati commessi, nel loro interesse o a loro vantaggio, da dirigenti o da sottoposti.

Si nota sin da subito la scelta di compromesso adottata dal legislatore, il quale decide di definire questa nuova forma di responsabilità come "amministrativa", anziché come penale; cerca di allentare le forti tensioni provenienti dal mondo imprenditoriale preoccupato per le ricadute economiche di questa riforma. La dottrina critica profondamente questa scelta, definendola una "truffa di etichette"; il legislatore denomina questa forma di responsabilità come amministrativa quando in realtà, analizzandone gli elementi costitutivi, ci si accorge, sin da subito, che nella sostanza è penale.

A tal proposito, la Corte di cassazione, chiamata a pronunciarsi sull'argomento, statuisce che detta nuova responsabilità, nominalmente amministrativa, dissimula la sua natura sostanzialmente penale, forse sottaciuta per non aprire delicati conflitti con i dogmi personalistici dell'imputazione criminale di rango costituzionale[186].

Sin dall'introduzione di questa nuova forma di responsabilità si è aperto un dibattito circa la sua natura che ha condotto la dottrina e la giurisprudenza a condividere unanimemente l'assenza di una vera e propria natura amministrativa. Le opinioni oscillano tra due diverse soluzioni: si tratta di una responsabilità penale mascherata da responsabilità amministrativa ovvero si tratta di un *tertium genus* rispetto alla responsabilità penale e alla responsabilità *ex* L. n. 689/1981 in tema di sanzioni amministrative pecuniarie. I fautori della prima teoria depongono in tal senso sulla base della circostanza che la responsabilità rimane agganciata alla commissione di una fattispecie propriamente penale, il suo accertamento avviene in sede di processo penale, la responsabilità *ex crimine* della persona giuridica è caratterizzata da autonomia[187], le

[184] Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300.

[185] Ratifica la Convenzione OCSE del 17 febbraio 1997, Parigi sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche internazionali.

[186] cfr. Cass. pen., sez. II, 30 gennaio 2006, n. 3615, sent.

[187] *Ex* art. 8 D. Lgs. 231/200: «*1. La responsabilità dell'ente sussiste anche quando: a) l'autore del*

disposizioni riportano istituti tipici del diritto penale e le sanzioni individuate provengono dall'area del diritto penale e sono caratterizzate da un'elevata afflittività. I fautori della seconda teoria, invece, pur in presenza dei dati oggettivi appena menzionati, sulla base di ragioni di ordine costituzionale, sostengono che si tratti di un terzo tipo di responsabilità, alternativo sia alla responsabilità amministrativa che a quella penale, in quanto non è possibile ascrivere una responsabilità penale ad un soggetto diverso dall'autore del fatto di reato ed è impossibile riferire stati psicologici, quali dolo e colpa, a persone giuridiche incapaci per loro natura di atteggiamenti volitivi colpevoli[188]. Si sostiene il *tertium genus*[189] sulla base del fatto che da un lato viene irrogata la sanzione penale per l'autore materiale dell'illecito, secondo le normali regole di imputazione del reato e, dall'altro lato si va ad irrogare una sanzione amministrativa a carico dell'ente nell'interesse o a vantaggio del quale l'autore ha agito. In tal senso si riallaccia la costante giurisprudenza della Corte europea dei Diritti dell'Uomo che da decenni, nell'ambito dell'applicazione degli artt. 6 e 7 della Convenzione EDU[190], ha individuato un concetto di materia penale di carattere sostanziale, che prescinde dall' "etichetta" attribuita alla tipologia di intervento sanzionatorio prevista nei diversi ordinamenti dei paesi che aderiscono alla Convenzione[191].

Per concludere, si ritiene che la responsabilità della persona giuridica configurata dal D. Lgs. 231/2001 possa essere definita come responsabilità amministrativa surrettiziamente penale, in tal senso per esprimere la tendenza generale, comunitaria ed internazionale, di assimilare progressivamente il modello di responsabilità penale e il modello di responsabilità amministrativa con l'intento di creare un sistema unitario,

---

*reato non è stato identificato o non è imputabile; b) il reato si estingue per una causa diversa dall'amnistia. 2. Salvo che la legge disponga diversamente, non si procede nei confronti dell'ente quando è concessa amnistia per un reato in relazione al quale è prevista la sua responsabilità e l'imputato ha rinunciato alla sua applicazione. 3. L'ente può rinunciare all'amnistia*».

[188] cfr. E. AMATI, op. cit., pp. da 9 a 11.

[189] In tali termini si è pronunciata la giurisprudenza, secondo la quale si deve considerare «*la responsabilità come tertium genus nascente dall'ibridazione della responsabilità amministrativa con i principi e i concetti propri della sfera penale*» (cit. Cass. pen., sez. un., 24 aprile 2014, n. 38343, sent.).

[190] L'art. 6 della CEDU si riferisce al "diritto a un equo processo" e l'art. 7 della CEDU a "*nulla poena sine lege*".

[191] cit. A. CADOPPI [et. al.], op. cit., pp. 194 e 195.

necessario per fronteggiare, con un'adeguata risposta punitiva, i fenomeni di criminalità economica.

Detta responsabilità si caratterizza per essere diretta, autonoma ed eventualmente concorrente con quella dell'autore del fatto. A giudizio della dottrina maggioritaria, infatti, si tratta di una responsabilità diretta, in quanto non soggetta ad alcuna condizione sospensiva, né caratterizzata da sussidiarietà rispetto a quella della persona fisica[192]. Si caratterizza per un'autonomia perché prescinde dall'accertamento della responsabilità della persona fisica autrice del fatto di reato[193]. È una responsabilità non accessoria rispetto a quella dell'autore individuale, in quanto, pur presupponendo la commissione di un reato da parte dell'autore individuale, la stessa non risulta condizionata dalla concreta punibilità di quest'ultimo.

La responsabilità amministrativa da reato dell'ente si delinea qualora una persona fisica, appartenente all'organico dell'ente e con esso legata da un rapporto funzionale, commette uno dei reati espressamente previsti dalla legge, c.d. reati presupposti, nell'interesse o a vantaggio dell'ente stesso; in aggiunta si richiede che vi sia il requisito soggettivo della "colpa di organizzazione", ovverosia l'ente risulta colpevole per non aver posto in essere determinati comportamenti che avrebbero permesso un controllo sufficiente per prevenire il reato commesso.

[192] Non sono mancate opinioni di segno opposto che valorizzando il profilo della derivazione della responsabilità dell'ente da quella del singolo autore del reato hanno evidenziato l'assenza, nel sistema delineato dal D. Lgs. 231/2001, di un'imputazione diretta a carico della società del fatto commesso a suo vantaggio o nel suo interesse (Così, M. ROMANO, *La responsabilità amministrativa degli enti, società o associazioni: profili generali,* in *Governo dell'impresa e mercato delle regole, Scritti giuridici per Guido Rossi*, vol. II, Milano, 2002).

[193] Secondo quanto dispone l'art. 8 del D. Lgs 231/2001.

## 3.2. *I requisiti e presupposti della responsabilità amministrativa da reato dell'ente*

### 3.2.1. *I soggetti destinatari della disciplina*

L'art. 1, comma 2 del D. Lgs. 321/2001 stabilisce che le disposizioni in esso previste si applicano: «*agli enti forniti di personalità giuridica e le società e associazioni anche prive di personalità giuridica*». Il legislatore ha optato per un'applicazione generalizzata, le disposizioni del Decreto si applicano sia agli enti personificati sia a quelli privi di personalità giuridica, superando definitivamente la tradizionale contrapposizione.

Sono esclusi dal campo di applicazione, *ex* art. 1, comma 3 del Decreto, lo Stato, gli enti pubblici territoriali (regioni, province e comuni)[194], gli altri enti pubblici non economici[195] nonché gli enti che svolgono funzioni di rilievo costituzionale[196]. Si tratta di categorie di soggetti non sempre del tutto chiare, questo porta a delle incertezze circa l'applicazione o meno del regime sanzionatorio, nel risolverle si propende per l'esclusione.

Vi sono incertezze anche rispetto alle imprese individuali, la giurisprudenza oscilla. Inizialmente, si escludeva l'applicabilità delle norme in esame, non essendoci una metà-individualità, successivamente si riconosce la responsabilità facendole rientrare nel concetto di "enti forniti di personalità giuridica"; anche se, quest'ultima impostazione sembrerebbe contraria al divieto di analogia in *malam partem* e il principio del *ne bis in idem* sostanziale[197].

---

[194] L' esenzione dall'applicazione del D. Lgs. 231/2001 di questi soggetti è coerente con quanto previsto all'art. 197 c.p. che li vede esclusi da ogni responsabilità solidale di natura civilistica per il pagamento della multa o dell'ammenda (cit. E. M. AMBROSETTI, E. MEZZETTI, M. RONCO, *Diritto penale dell'impresa*, V ed., Zanichelli, Bologna, 2022, p. 56).

[195] Per la Legge delega 300/2000, l'esclusione avrebbe dovuto essere prevista soltanto per gli enti che esercitano pubblici poteri e gli enti pubblici non economici non esercitano pubblici poteri; quindi, avrebbero dovuto essere assoggettati alla disciplina. Gli enti pubblici destinatari della disciplina in esame sono solo quelli economici ovvero coloro che *ex* art. 2201 c.c. «*hanno per oggetto esclusivo o principale un'attività commerciale*» (cit. E. M. AMBROSETTI [et. al.], op. cit., pp. 56 e 57).

[196] Ci si riferisce a: Camera dei Deputati, Corte Costituzionale, Senato, Segretariato generale della Presidenza della Repubblica, Senato, C.s.m., C.n.e.l. e si ritiene anche i partiti politici e sindacali.

[197] Il divieto di analogia *in malam partem* è previsto all'art. 14 delle disposizioni sulla legge in generale che vieta il ricorso al procedimento analogico per le norme penali. Trova fondamento costituzionale come corollario del principio di legalità all'art. 25, comma 2 Cost. in base al quale le norme non si applicano al di fuori dei casi da esse stesse espressamente stabiliti, con l'obbiettivo di assicurare la

Infine, rispetto ad un gruppo societario, la Cassazione penale, sez. II, il 27 settembre e 9 dicembre 2016, con la sentenza n. 52316 stabilisce: «*Il fatto che, formalmente, le società facenti parte del gruppo siano giuridicamente autonome ed indipendenti, non impedisce che le attività di ciascuna costituiscano espressione di una comune politica d'impresa, generalmente voluta dalla holding*[198] *partecipate nell'ottica della diversificazione dei rischi*», per cui la società capogruppo può «*essere chiamata a rispondere per il reato commesso nell'ambito dell'attività di una società controllata laddove il soggetto agente abbia perseguito anche un interesse riconducibile alla prima*».

La commissione materiale del reato viene posta in essere da una persona fisica, facente parte dell'organico dell'ente, che si differenzia in base alla posizione rivestita. Si parla di soggetto apicale per indicare coloro che fanno parte della rappresentanza, amministrazione, direzione ovvero gestione o controllo di fatto dell'ente; mentre, si parla di soggetto sottoposto per identificare coloro che sono in un rapporto di dipendenza da persone in posizione apicale[199]. Tra l'autore del reato e l'ente vi è un rapporto funzionale, il quale varia a seconda delle posizioni appena viste ed influenza i criteri di imputazione

---

garanzia della libertà dell'individuo contro possibili arbitrarie limitazioni della libertà personale al di là delle ipotesi espressamente previste dal legislatore; pertanto, non si preclude l'applicazione analogica di norme penali che determinano un trattamento favorevole al reo, ma solo di quelle incriminatrici ovvero che aggravano il trattamento sanzionatorio (cit. *Analogia: legis e iuris*, in *diritto.it*, Network Maggioli editore, 2018). Il principio del *ne bis in idem* sostanziale consiste nel divieto che il medesimo fatto possa essere addebitato più volte allo stesso soggetto, qualora l'applicazione di una sola delle norme in cui il fatto è sussumibile ne esaurisca, per intero, il contenuto di disvalore sia da un punto di vista oggettivo, che soggettivo. Dunque, è inammissibile, a fronte di un medesimo fatto, la doppia sanzione, ogniqualvolta la natura del reato, il bene giuridico tutelato e l'evento, esauriscano integralmente il disvalore della condotta, tanto rispetto alla tipicità del fatto che sotto il profilo soggettivo. Tale concetto si differenzia dal divieto di *ne bis in idem* processuale previsto all'art. 649 c.p. che si sostanzia nel divieto di un secondo giudizio per il medesimo fatto (cit. P. BALBONI, F. TUGNOLI, *Reati informatici e tutela dei dati personali: profili di responsabilità degli enti*, in *Giurisprudenza penale web*, 1-*bis*, 2021, p. 24, nota 52).

[198] Il termine inglese *holding* è l'abbreviazione di *holding company*, con cui si designa una società finanziaria (capogruppo o madre) che detiene una parte, o la totalità, del capitale di altre imprese, che possono avere per oggetto settori economici diversi ovvero distinte fasi dello stesso processo produttivo, al fine di controllarne la gestione finanziaria, industriale e commerciale (cit. Enciclopedia online, in *treccani.it*).

[199] *Ex* art. 5 del D. Lgs. 231/2001: «1. *L'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio: a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso; b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a). 2. L'ente non risponde se le persone indicate nel comma 1 hanno agito nell'interesse esclusivo proprio o di terzi*».

della responsabilità all'ente stesso. Nel caso in cui l'autore del reato sia un soggetto in posizione apicale la responsabilità dell'ente risulta essere tendenzialmente automatica ed assoluta; di converso, nel caso in cui l'autore sia un soggetto sottoposto all'altrui direzione, l'ente risponderà solo qualora sia riscontrabile un'agevolazione colposa[200].

### 3.2.2. *Le nozioni di "interesse" e "vantaggio"*

Le persone fisiche appena dette commettono l'illecito nell'interesse o a vantaggio dell'ente[201]. Si tratta di un importante criterio di imputazione, per cui l'ente non risulta responsabile qualora il soggetto abbia agito nell'interesse proprio o di terzi. Secondo la tesi dominante, interesse e vantaggio sono criteri alternativi ed indipendenti; quando si parla di interesse si esprime una valutazione teleologica del reato, apprezzabile *ex ante*, al momento della commissione del fatto e secondo un metro di giudizio soggettivo in relazione all'elemento psicologico dell'autore dell'illecito; mentre, il criterio del vantaggio ha una connotazione essenzialmente oggettiva, come tale valutabile *ex post*, sulla base degli effetti concretamente derivanti dalla realizzazione del reato. In sintesi, per configurare la responsabilità dell'ente è sufficiente che venga provato che lo stesso abbia ricavato dal reato un vantaggio anche quando non è stato possibile determinare l'effettivo interesse vantato *ex ante* alla consumazione dell'illecito[202].

A tal proposito, bisogna ricordare un problema interpretativo nato a seguito dell'introduzione di nuovi reati c.d. presupposto rientranti nella fattispecie colposa, in particolare, i reati ambientali e in materia di sicurezza del lavoro. In merito, appare spontanea la domanda, qual è l'interesse o il vantaggio che l'ente riceverebbe nel caso, per esempio, dalla morte di un lavoratore a seguito di un infortunio sul lavoro? Si tratta

[200] Quando si parla di agevolazione colposa ci si riferisce alla rilevanza penale che assume, non solo la condotta di partecipazione che rende possibile la perpetrazione del fatto, ma anche quella condotta che, alla stregua di un giudizio *ex post*, si limita a facilitarne o agevolarne la realizzazione (cit. G. FIANDACA, E. MUSCO, op. cit., p. 529).

[201] *Ex* art. 5 del D. Lgs. 231/2001.

[202] cit. A. CADOPPI [et. al.], op. cit., p. 196.

di omicidio colposo commesso dai soggetti dirigenti a seguito di una violazione delle norme in materia di sicurezza e salute sul lavoro. A questa domanda è stata la Sentenza della Cassazione, sez. un., 24 aprile 2014, n. 38343, c.d. *ThyssenKrupp*[203] a dare una risposta. La Cassazione ha affermato che, per accertare l'interesse o il vantaggio dell'ente, attraverso una valutazione oggettiva, bisogna guardare il momento antecedente rispetto all'evento in quanto tale, ovvero il risparmio di spesa che l'ente può aver ottenuto nell'ipotesi in cui non abbia rispettato le regole in materia di salute e sicurezza sul lavoro e di conseguenza l'interesse sarebbe stato il risparmio sui presidi di sicurezza. Quindi, la giurisprudenza di merito affermò il collegamento dell'interesse o del vantaggio alla condotta dei delitti di omicidio e lesioni colpose, per violazione delle norme cautelari a tutela della sicurezza e della salute sul lavoro.

Si vede come in alcuni casi l'interesse viene inteso in senso oggettivo, essendo sufficiente che la condotta sia stata realizzata nel contesto di un'attività propria dell'ente e che l'autore non abbia agito nel suo esclusivo interesse; mentre, in altri casi viene concepito soggettivamente, ovvero come finalità soggettiva dell'autore di realizzare un interesse esclusivo dell'ente.

La Sentenza Cass., sez. un., 24 aprile 2014, n. 38343 recita, relativamente ai

---

[203] Il fatto, in breve: nel dicembre del 2007, nello stabilimento torinese delle acciaierie *ThyssenKrupp*, vi fu un incendio nel quale persero la vita sette dipendenti. Emerse, all'epoca, un complessivo degrado dell'impianto, sostanzialmente dovuto alla decisione della Società di dismetterlo per trasferire gli impianti a Terni, con conseguente cessazione degli investimenti per la sicurezza nella sede di Torino. In particolare, furono rilevate significative carenze nella manutenzione e molteplici violazioni di misure antinfortunistiche, che contribuirono a determinare il devastante incendio. L'amministratore delegato della società fu accusato e condannato dalla Corte di Assise di Torino per omicidio volontario dei lavoratori *ex* art. 575 c.p., ritenendosi sussistente in capo allo stesso l'elemento soggettivo del dolo eventuale, in quanto, essendo a conoscenza delle condizioni di insicurezza dello stabilimento, non aveva attuato le doverose misure, decidendo di posticipare l'investimento antincendio. Nel successivo giudizio di appello, la sentenza venne parzialmente riformata dalla Corte di Assise di Appello di Torino la quale, diversamente, qualificò il fatto come omicidio colposo aggravato dalla colpa cosciente. La "colpa cosciente" rappresenta una specifica ipotesi aggravata dei delitti colposi e si configura per "avere agito nonostante la previsione dell'evento". Avverso tale sentenza il Procuratore Generale presentò impugnazione, insistendo, affinché la fattispecie venisse riconosciuta come dolosa, in considerazione delle esistenti divergenze giurisprudenziali sull'individuazione della linea di confine tra dolo eventuale e colpa cosciente. Tenuto conto dell'estrema importanza della questione e della necessità di un definitivo chiarimento, il ricorso venne assegnato alla Suprema Corte a Sezioni Unite che, con sentenza n. 38343/14 del 24 aprile 2014, depositata in data 18 settembre 2014, ha infine posto un punto fermo sulla questione, riconducendo la responsabilità dell'amministratore per la vicenda di cui trattasi nell'alveo della "colpa cosciente".

concetti di interesse e vantaggio: «*vanno di necessità riferiti alla condotta e non all'esito antigiuridico*» essendo possibile che «*una condotta caratterizzata dalla violazione della disciplina cautelare e quindi colposa sia posta in essere nell'interesse dell'ente o determini comunque il conseguimento di un vantaggio*», si tratta di un criterio interpretativo che «*si limita ad adottare l'originario criterio di imputazione al mutato quadro di riferimento, senza che i criteri d'ascrizione ne siano alteranti. L'adeguamento riguarda solo l'oggetto della valutazione, che coglie non più l'evento bensì solo la condotta, in conformità alla diversa conformazione dell'illecito; e senza, quindi un vulnus ai principi costituzionali dell'ordinamento penale. Tale soluzione non presenta incongruenze: è ben possibile che l'agente violi consapevolmente la cautela, o addirittura preveda l'evento che ne può derivare, pur senza volerlo, per corrispondere ad istanze funzionali a strategie dell'ente. A maggior ragione vi è perfetta compatibilità tra inosservanza della prescrizione cautelare ed esito vantaggioso per l'ente*».

In sintesi, i concetti di interesse e vantaggio si devono riferire alla condotta e no all'evento, sono criteri di imputazione oggettiva concorrenti ed alternativi; l'interesse si valuta *ex ante*, al momento della commissione del fatto e con un giudizio soggettivo, mentre il vantaggio ha una connotazione oggettiva e si valuta *ex post*, sulla base degli effetti derivati dal reato. Per concludere, vi è interesse se l'autore viola consapevolmente le norme cautelari per conseguire un'utilità per l'ente; mentre, sussiste il vantaggio qualora l'autore abbia violato le norme prevenzionistiche, per ridurre i costi e contenere la spesa, indipendentemente dalla volontà di ottenerne un vantaggio.

### 3.2.3. *I reati presupposto*

L'ente sarà responsabile solo nel caso in cui la persona fisica commetta uno dei reati previsti dal Decreto, detti anche reati presupposto, nel rispetto del principio di legalità previsto all'art. 2[204].

[204] *Ex* art. 2 del D. Lgs. 231/2001: «*L'ente non può essere ritenuto responsabile per un fatto*

L'obbiettivo auspicato consisteva nel colpire tutti i settori dove generalmente si manifesta la criminalità d'impresa. Il legislatore inizialmente mantenne un atteggiamento prudente, che destava non poche perplessità, successivamente, grazie a diversi interventi aggiuntivi ha progressivamente esteso il novero dei reati presupposto. Ad oggi, il catalogo normativo appare, complessivamente, in linea con le attuali esigenze politico-criminali.

In breve, il catalogo dei c.d. reati presupposto, si compone da: i reati contro la pubblica amministrazione; i reati contro la fede pubblica; i reati con finalità di terrorismo e di eversione dell'ordine democratico; i reati contro l'ordine pubblico; i reati contro la persona; i reati contro la personalità individuale; i reati informatici; i reati contro il patrimonio; infine, i reati contro l'industria e il commercio.

### 3.2.4. *La colpa per organizzazione*

Per procedere all'attribuzione ad una persona giuridica della responsabilità amministrativa da reato è necessario verificare la sussistenza dei criteri di imputazione soggettivi. Perciò, la commissione da parte di una persona fisica di uno dei reati c.d. presupposto, nell'interesse o a vantaggio dell'ente, è requisito necessario, ma non sufficiente: affinché sorga la responsabilità aggiuntiva dell'ente occorre che il reato commesso sia ad esso riconducibile anche sotto il profilo soggettivo.

Risulta pacifica per la giurisprudenza la necessità di individuare una colpevolezza dell'ente, la quale non può essere mutuata secondo i criteri tradizionali del diritto penale, chiaramente incompatibili con la persona giuridica. Si cerca di costruire una forma di colpevolezza diversa, secondo la teoria prevalente, all'ente è ascrivibile una colpa per organizzazione.

L'ente non può essere colpevole per il reato in quanto tale, non potendo essere

---

*costituente reato se la sua responsabilità amministrativa in relazione a quel reato e le relative sanzioni non sono espressamente previste da una legge entrata in vigore prima della commissione del fatto*».

negligente, imprudente o imperito, il reato viene materialmente commesso da una persona fisica facente parte dell'organico interno che compone l'ente stesso e la quale risulta imputabile soggettivamente secondo i criteri tradizionali.

Quindi, si immagina una colpevolezza concepita sempre come rimproverabilità soggettiva, in modo da essere compatibile con l'art. 27 Cost., ma connessa al fatto; come si legge nella Relazione ministeriale al D. Lgs. 231/2001: «*Il reato dovrà costituire anche espressione della politica aziendale o quantomeno derivare da una colpa di organizzazione* […]. *All'ente viene in pratica richiesta l'adozione di modelli comportamentali specificatamente calibrati sul rischio-reato, e cioè volti ad impedire, attraverso la fissazione di regole di condotta, la commissione di determinati reati. Requisito indispensabile perché dall'adozione del modello derivi l'esenzione da responsabilità dell'ente è che esso venga efficacemente attuato: l'effettività rappresenta, dunque, un punto qualificante ed irrinunciabile del nuovo sistema di responsabilità*»[205].

In sostanza si delinea una colpa anticipata, per cui l'ente è colpevole per non aver organizzato la realtà al suo interno, secondo le modalità previste dal D. Lgs. 231/2001[206] che sarebbero state in grado di evitare la commissione di illeciti. Si rimprovera all'ente di non aver strutturato un'organizzazione interna con controlli e procedure idonee ad evitare la commissione di reati.

### 3.2.5. *Art. 6 e art. 7 del D. Lgs. 231/2001*

Fondamentale è ricordare che il rapporto funzionale, che lega l'ente ai soggetti in posizione apicale ovvero ai sottoposti, influenza i criteri di imputazione della responsabilità all'ente stesso. Ai sensi dell'art. 6 del Decreto il legislatore, partendo dal presupposto che i soggetti apicali agiscono secondo la volontà dell'impresa, prevede un'inversione dell'onere della prova, per cui sarà l'ente, per non essere considerato

[205] cit. *Relazione ministeriale al D. Lgs. 231/2001*, pp. 8 e 9, consultabile sul sito *osservatorio 231.it*.

[206] Ci si riferisce a tutti gli elementi previsti espressamente dal D. Lgs. 231/2002 agli artt. 6 e 7 che, se adottati nell'organizzazione interna di ente, prevengono ed evitano la commissione di reati.

responsabile, a dover dimostrare che: «[…] *a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi; b) il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo; c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione; d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b)*. […]».

Per quanto attiene al reato commesso dai soggetti sottoposti all' altrui direzione, ai sensi dell'art. 7 del Decreto l'ente sarà responsabile «[…]*se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza*», prosegue al comma 2: «*In ogni caso, è esclusa l'inosservanza degli obblighi di direzione o vigilanza se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi* […]». Quindi, l'adozione di Modelli organizzativi sembrerebbe mettere al riparo l'ente da eventuali responsabilità.

Rispetto a detti articoli si possono notare alcune peculiarità relativamente al nesso causale tra l'inosservanza degli obblighi di vigilanza e la commissione del reato. Qualora il reato venga commesso dai vertici, l'ente, che non ha predisposto i Modelli di organizzazione, rinuncia *a priori* alla possibilità di andare esente da responsabilità. Diversamente, nell'ipotesi di condotta illecita da parte di un dipendente, la mancanza di tali Modelli non comporta necessariamente la sanzione amministrativa; infatti, pur essendo l'ente privo di Modelli di organizzazione, questa carenza potrebbe non risultare connessa eziologicamente al reato commesso[207].

Inoltre, si possono ravvisare due tipi di illecito strutturalmente diversi, nel fatto-reato commesso da un soggetto apicale vi è una responsabilità concorrente dell'ente; mentre, nel fatto-reato commesso da un dipendente si crea una fattispecie complessa che corrisponde ad un fatto di agevolazione colposa dell'altrui reato.

[207] cit. E. M. AMBROSETTI [et. al.], op. cit., p. 67.

Gli articoli appena visti[208] prevedono delle clausole di esonero dalla responsabilità amministrativa da reato, quando l'ente adotta ed attua, prima della commissione del reato, un Modello di organizzazione, gestione e controllo, anche detto "MOGC", efficiente e, in aggiunta, sussistono i requisiti previsti agli artt. 6 e 7 del Decreto. Si applica la scusante[209], nel caso in cui il reato sia commesso da un soggetto apicale; mentre, qualora il reato sia commesso da un sottoposto ciò implica la mancanza di un elemento essenziale dell'illecito attribuito all'ente collettivo, per cui il fatto non costituisce reato.

Per quanto attiene al caso di responsabilità penale della persona che riveste una posizione apicale, nel caso in cui l'ente adotti un MOGC efficiente, per un reato commesso da un sottoposto, vi sono opinioni divergenti. Vi è chi ritiene che appaia difficile ipotizzare una responsabilità del dirigente per omesso impedimento dell'evento reato, stante la necessità di accertare una causalità omissiva; di converso, vi è chi sostiene che una volta introdotti questi Modelli di gestione ed organizzazione, è obbligo del dirigente attuarli e rispettarli e l'inosservanza di detto obbligo potrebbe rilevare giuridicamente ai sensi dell'art. 40, comma 2 c.p.[210].

In breve, il Modello di organizzazione, gestione e controllo adottato ed approvato dal Consiglio di amministrazione, dev'essere idoneo ed efficacemente attuato, affinché si possa prevenire la commissione di reati; gli elementi essenziali sono disciplinati all'art. 6, comma 2 e all'art. 7 comma 3[211].

---

[208] Ci si riferisce all'art. 6 e 7 del D. Lgs. 231/2001.

[209] A tal proposito vi sono differenti orientamenti: secondo un primo orientamento, si è affermato che, ragionando secondo le categorie della teoria del reato, le fattispecie di esonero andrebbero collocate non nella sfera delle scusanti soggettive, bensì in quella "residuale" della punibilità; in base ad una diversa ricostruzione, la prova dell'adeguata vigilanza di cui all'art. 6, si atteggerebbe a vera e propria scusante rispetto ad una fattispecie di responsabilità già di per sé integrata sulla base del reato commesso dall'apice nell'interesse dell'ente (cit. E. M. AMBROSETTI [et. al.], op. cit., p. 73).

[210] Così, A. GARGANI, *Imputazione del reato agli enti collettivi e responsabilità penale dell'intraneo: due piani irrelati?*, in *Diritto penale e processo*, 2002, p. 1066.

[211] *Ex* art. 6, comma 2 del D. Lgs. 231/2001: «*In relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, i modelli di cui alla lettera a), del comma 1, devono rispondere alle seguenti esigenze: a) individuare le attività nel cui ambito possono essere commessi reati; b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire; c) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati; d) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli; e) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello*». *Ex* art. 7, comma 3 del D. Lgs. 231/2001: «*Il modello prevede, in relazione alla natura e alla dimensione dell'organizzazione nonché al tipo di attività*

### 3.2.6. *Il principio di autonomia*

L'art. 8 del Decreto introduce il principio di autonomia della responsabilità dell'ente, il quale prevede che la responsabilità sussiste anche se «*l'autore del reato non è stato identificato o non è imputabile*», nonché se «*il reato si estingue per causa diversa dall'amnistia*». Il legislatore adotta questa disciplina per ragioni di opportunità, posto che non vi è una disciplina specifica nel caso in cui la complessità della compagine sociale non consenta di identificare il reo[212]. Vi sono una serie di dubbi in merito a tale principio, se vi è incertezza circa l'autore del reato viene logicamente compromessa la piena verifica dell'elemento psicologico, dolo o colpa. Dunque, si tratta di una responsabilità amministrativa dell'ente attribuita nonostante l'impossibilità, a priori, di accertare l'elemento psicologico del reato.

Qualche autore sostiene che il presupposto della responsabilità amministrativa dell'ente sia la commissione di un mero fatto-reato, non essendo necessario valutare la sussistenza dell'elemento psicologico. Tuttavia, appare scorretto considerare detta norma come generale, poiché disciplina un'ipotesi particolare ed eccezionale; la responsabilità dell'ente è considerata autonoma, ma anche aggiuntiva rispetto a quella dell'autore materiale del reato, perciò, è obbligatorio l'accertamento di tutti gli elementi del reato, compresi quelli soggettivi.

Inoltre, come prima accennato, l'art. 8, comma 1, lett. b) del D. Lgs. 231/2001 stabilisce come la responsabilità dell'ente sussista anche quando «*il reato si estingue per una causa diversa dall'amnistia*», si afferma che tutte le cause di estinzione del reato non escludono la responsabilità amministrativa dell'ente[213]. Collegate a tale disposizione ve ne sono altre che ne restringono fortemente la portata, per evitare di ricadere

*svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio*».

[212] cit. E. M. AMBROSETTI [et. al.], op. cit., p. 74.

[213] cfr. Cass. pen., sez. VI, 25 gennaio 2013, n. 21192, sent. nella quale si sottolinea il fatto che l'intervenuta estinzione del reato presupposto per prescrizione non fa venir meno l'autonomo percorso processuale della responsabilità dell'ente, anche se non si può prescindere una verifica circa la sussistenza del fatto di reato, quale elemento costitutivo della responsabilità amministrativa da reato della persona giuridica.

nell'interpretazione secondo la quale la responsabilità dell'ente è conseguenza di un mero fatto di reato. L'art. 59 del Decreto esclude espressamente che possa contestarsi un reato qualora vi sia stata l'archiviazione; perciò, la causa di estinzione, costituendo una causa di archiviazione ai sensi dell'art. 411 c.p.p.[214], impedirà anche la contestazione del reato a carico della persona giuridica. Anche l'art. 60 limita la disposizione dell'art. 8, comma 1, lett. b), stabilendo che «*non può procedersi alla contestazione di cui all'art. 59 quando il reato da cui dipende l'illecito amministrativo dell'ente è estinto per prescrizione*»; quindi, il potere di contestazione rimane quando la prescrizione matura a contestazione avvenuta; anche in tal caso la responsabilità dell'ente potrebbe nascere a prescindere dalla verifica della colpevolezza del reo, questo ove il reato si prescriva nelle more del processo penale.

### 3.2.7. *La delega di funzioni*

Nell'ambito degli enti collettivi o delle imprese, non è sempre agevole individuare il soggetto persona fisica autore del reato, questo perché non sempre il soggetto formalmente titolare degli obblighi di condotta penalmente sanzionati è in grado di adempiervi personalmente: ciò induce il titolare originario a delegare l'adempimento di detti obblighi ad altri soggetti. Quindi, il problema che sorge è se il fenomeno della delega possa assumere rilevanza penale, sia rispetto ad un'esenzione da responsabilità del titolare originario, sai rispetto all'attribuzione della responsabilità in capo al nuovo soggetto di

[214] *Ex* art. 411 c.p.p.: «*1. Le disposizioni degli articoli 408, 409, 410 e 410-bis si applicano anche quando risulta che manca una condizione di procedibilità, che la persona sottoposta alle indagini non è punibile ai sensi dell'articolo 131-bis del codice penale per particolare tenuità del fatto che il reato è estinto o che il fatto non è previsto dalla legge come reato [125 disp. att.]. 1-bis. Se l'archiviazione è richiesta per particolare tenuità del fatto, il pubblico ministero deve darne avviso alla persona sottoposta alle indagini e alla persona offesa, precisando che, nel termine di dieci giorni, possono prendere visione degli atti e presentare opposizione in cui indicare, a pena di inammissibilità, le ragioni del dissenso rispetto alla richiesta. Il giudice, se l'opposizione non è inammissibile, procede ai sensi dell'articolo 409, comma 2, e, dopo avere sentito le parti, se accoglie la richiesta, provvede con ordinanza. In mancanza di opposizione, o quando questa è inammissibile, il giudice procede senza formalità e, se accoglie la richiesta di archiviazione, pronuncia decreto motivato. Nei casi in cui non accoglie la richiesta il giudice restituisce gli atti al pubblico ministero, eventualmente provvedendo ai sensi dell'articolo 409, commi 4 e 5».*

fatto preposto all'adempimento. A tal proposito, vi è stato il D. Lgs. 81/2008[215], quale esito di una lunga evoluzione giurisprudenziale e dottrinale, il quale all'art. 16 prevede: «*1. La delega di funzioni da parte del datore di lavoro, ove non espressamente esclusa, è ammessa con i seguenti limiti e condizioni: a) che essa risulti da atto scritto recante data certa; b) che il delegato possegga tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate; c) che essa attribuisca al delegato tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate; d) che essa attribuisca al delegato l'autonomia di spesa necessaria allo svolgimento delle funzioni delegate; e) che la delega sia accettata dal delegato per iscritto. 2. Alla delega di cui al comma 1 deve essere data adeguata e tempestiva pubblicità. 3. La delega di funzioni non esclude l'obbligo di vigilanza in capo al datore di lavoro in ordine al corretto espletamento da parte del delegato delle funzioni trasferite. La vigilanza si esplica anche attraverso i sistemi di verifica e controllo di cui all'articolo 30, comma 4*». Da sottolineare, è l'obbligo di vigilanza che, in ogni caso, incombe sui soggetti deleganti, delineato dettagliatamente all'art. 30, comma 4 del D. Lgs. 81/2008, per cui i Modelli organizzativi e gestionali adottati devono prevedere anche un idoneo sistema di controllo sull'effettiva attuazione di tutte le misure di carattere precauzionale. Anche se il Decreto riferisce l'obbligo di sorveglianza all'adempimento delle misure di controllo incluse nel MOG, nondimeno è possibile ritenere che un dovere di vigilanza residui anche in capo ai soggetti deleganti che operino in imprese non dotate di detti Modelli, sulla base del principio condiviso per cui la delega non libera il titolare originario dalla responsabilità, ma implica un dovere di controllo sugli adempimenti incombenti sul soggetto delegato, in modo da evitare un indebito slittamento verso il basso della responsabilità penale[216].

[215] In Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro.

[216] cit. G. FIANDACA, E. MUSCO, op. cit., p. 188.

### 3.2.8. *Il sistema sanzionatorio*

Il sistema sanzionatorio delineato dal D. Lgs. 231/2001 si rivolge all'ente e non alla persona fisica, risulta essere particolarmente afflittivo e si caratterizza per due tipi di sanzioni, pecuniarie ed interdittive, alle quali si aggiungono la confisca e la pubblicazione della sentenza di condanna.

Le pene per gli illeciti amministrativi dipendenti da reato, nel testo normativo, vengono indicate come "sanzioni amministrative"[217], tuttavia è ancora vivo in dottrina il dibattito sulla loro natura giuridica[218].

Le sanzioni pecuniarie sono previste sempre, per tutti gli illeciti in cui sorge la

[217] In tal senso la rubrica dell'art. 9 del D. Lgs. 231/2001.

[218] Vi è chi le considera alla stregua di sanzioni penali sulla base di una serie di argomentazioni: con riguardo a tali sanzioni è prevista la responsabilità diretta dell'ente (cioè per fatto proprio dell'ente, nel caso di reato commesso da soggetto in posizione apicale); la competenza del giudice penale; il procedimento per l'accertamento dei reati, che ricalca per lo più quello previsto dal codice di procedura penale; la previsione di cui all'art. 3 del D. Lgs. 231/2001, che sancisce l'applicabilità della disciplina più favorevole in caso di successione di leggi nel tempo; l'esclusione della facoltà per l'ente di pagare la sanzione pecuniaria in misura ridotta; la competenza del Pubblico Ministero ad effettuare la contestazione del reato (In tal senso C. E. PALIERO, *Il d.lgs. 8 giugno 2001 n. 231: da ora in poi, societas delinquere (et puniri) potest*, in *Corriere giuridico*, 2001; E. MUSCO, *Le imprese a scuola di responsabilità tra pene pecuniarie e misure interdittive,* in *Diritto e giustizia*, n. 23, 2001, p. 8). Di converso vi è chi le interpreta come sanzioni amministrative sulla base degli insormontabili problemi di compatibilità con l'art. 27 Cost., nel quale si considera la colpevolezza in senso "psicologico", come legame psichico tra fatto e autore (Come interpreta la Corte Costituzionale nella Sentenza n. 456/1998, secondo la quale «*le sanzioni penali possono riguardare solo le condotte individuali, le uniche assoggettabili a pena in forza del principio di personalità della responsabilità penale*»), inoltre la struttura degli enti non permetterebbe di perseguire le finalità rieducative della pena. A favore della natura amministrativa vi sono le seguenti argomentazioni: la sussistenza in capo all'ente, relativamente alla commissione dei reati presupposto da parte dei soggetti in posizione apicale, di una presunzione di colpevolezza, per cui l'ente deve provare la mancanza di colpevolezza per sottrarsi all'applicazione delle sanzioni; la competenza del Pubblico Ministero a disporre l'archiviazione ove ne ricorrono le condizioni; la mancanza di una disposizione che preveda espressamente il principio del cumulo di responsabilità dell'ente con quella della persona fisica; la circostanza che il reato della persona fisica è una condizione logica-giuridica rispetto all'accertamento dell'illecito dell'ente.
Infine, vi è chi interpreta le sanzioni previste nel D. Lgs. 231/2001 come un *tertium genus*, una via di mezzo tra le sanzioni penali e le sanzioni amministrative, in linea con l'esigenza espressa nella Relazione ministeriale al decreto che prevede di «*omogeneizzare i sistemi di responsabilità amministrativa e di responsabilità penale all'insegna delle massime garanzie previste per quest'ultimo, spingendo verso la progressiva assimilazione dei due modelli, che tendono a confluire in una sorta di "diritto sanzionatorio" unitario, soprattutto in materia economica*».

responsabilità da reato dell'ente[219]; mentre, le sanzioni interdittive si applicano solo se espressamente previste per lo specifico reato presupposto commesso e in aggiunta alla sanzione pecuniaria.

Per quanto riguarda le sanzioni interdittive, nei casi più gravi comportano l'interdizione dall'esercizio dell'attività, mentre nei casi meno gravi implicano il divieto di pubblicizzare beni o servizi, di contrattare con la pubblica amministrazione o l'esclusione da agevolazioni, finanziamenti, sussidi, etc.

Si ritiene che le sanzioni interdittive debbano applicarsi solo in casi di maggiore gravità, quando ricorre almeno una delle condizioni previste all'art. 13 del D. Lgs. 231/2001, secondo le quali: l'ente ha tratto un profitto di rilevante gravità; il reato è stato commesso da soggetti in posizione apicale ovvero da soggetti sottoposti all'altrui direzione quando, in questo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative; infine, nel caso di reiterazione degli illeciti.

Qualora sussistano le condizioni per l'irrogazione di una sanzione interdittiva che determina l'interruzione dell'attività dell'ente, il giudice, può sostituirla con la nomina di un Commissario giudiziale[220].

Le sanzioni interdittive non possono essere applicate qualora, prima della dichiarazione di apertura del dibattimento di primo grado, l'ente faccia il necessario per garantire una riparazione dell'offesa, provvedendo al risarcimento del danno, o riparando le conseguenze dannose o pericolose del reato, o si attivi efficacemente in tal senso, o metta a disposizione, ai fini della confisca, il profitto conseguito, ovvero abbia eliminato le carenze organizzative causa del reato.

La sanzione pecuniaria si applica secondo il "sistema delle quote", il cui numero è stabilito dal giudice all'interno della cornice fissata dal Decreto rispetto a ciascun illecito, ma il cui importo è computato proporzionalmente alle condizioni economiche e

[219] A tal proposito si rileva che detto sistema possa essere eccessivamente gravoso nei confronti delle piccole aziende, le quali avendo delle ristrette dimensioni non permettono un vero discrimine tra azienda e titolare della medesima; perciò, l'irrogazione della sanzione pecuniaria all'ente, dopo che l'autore del reato è già stato punito, rischia di violare il *ne bis in idem* sostanziale, posto che si punisce due volte, per lo stesso fatto, un identico centro di interessi (cit. C. PIERGALLINI, *Sistema sanzionatorio e reati previsti dal codice penale*, Ipsoa, Milano, 2001, p. 1358).

[220] *Ex* art. 15 del D. Lgs. 231/2001.

patrimoniali della singola società e assoggettato alla confisca del prezzo profitto o prezzo del reato[221]. Il risultato di questo procedimento bifasico è l'applicazione di una sanzione proporzionata al disvalore oggettivo e soggettivo dell'illecito e anche commisurata alla capacità patrimoniale della persona giuridica.

Per quanto attiene alla pubblicazione della sentenza, l'art. 18 del D. Lgs. 231/2001 prevede: «1. *La pubblicazione della sentenza di condanna può essere disposta quando nei confronti dell'ente viene applicata una sanzione interdittiva.* 2. *La pubblicazione della sentenza avviene ai sensi dell'articolo 36 del codice penale nonché mediante affissione nel comune ove l'ente ha la sede principale*. 3. *La pubblicazione della sentenza è eseguita, a cura della cancelleria del giudice, a spese dell'ente*», in questo caso saltano agli occhi i riverberi reputazionali.

La confisca può essere diretta o per equivalente e va disposta altresì quando l'ente prova la propria non colpevolezza, se ha tratto profitto dalla commissione del reato[222]. La confisca per equivalente di somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato, si applica qualora la confisca diretta non sia possibile ed assolve una funzione compensatoria dell'equilibrio economico alterato dal reato, i cui effetti si sono verificati a vantaggio dell'ente[223].

Sia le sanzioni interdittive che la confisca possono essere applicate dal giudice in via cautelare come strumento di prevenzione generale immediatamente applicabile.

---

[221] cit. A. CADOPPI [et. al.], op. cit., p. 199.

[222] Il Codice penale non fornisce una definizione del "profitto" del reato e, tuttavia, tale concetto viene richiamato in diverse norme incriminatrici quali, ad esempio, il peculato, il furto, la rapina ed in tema di confisca *ex* artt. 240, 322 ter c.p. L'assenza di una definizione di "profitto" ha condotto la giurisprudenza ad una sua elaborazione distinguendolo, al contempo, dalle figure affini quali il "prezzo" ed il "prodotto" del reato. Secondo l'orientamento maggioritario in giurisprudenza per "profitto" si intende quell'entità suscettibile di valutazione economica eziologicamente connessa alla commissione di un reato. Viceversa, il "prezzo" del reato, pur costituendo anch'esso un'utilità economica, non deriva direttamente dalla commissione di un reato, bensì dalla condotta di un terzo. Per "prodotto" del reato si intende qualsiasi utilità, anche non avente valore economico, generata dalla sua commissione (cit. G. MARINO, *Il profitto del reato alla luce della teoria generale del reato e la sua rilevanza in tema di confisca. Il profitto, il prodotto ed il prezzo del reato: analisi dogmatica*, in *Altalex*, 2023).

[223] cfr. Cass. pen., sez VI, 24 gennaio 2014, n. 3635, sent.

### 3.3. *Profili di responsabilità degli enti nei reati informatici e nel trattamento illecito di dati* ex *art. 24-bis D. Lgs. 231/2001*

Nelle realtà aziendali si deve affrontare una problematica molto diffusa e pericolosa: il *cyberattack*. Per *cyberattack* ci si riferisce alle varie modalità di attacco alla sicurezza delle informazioni di un'organizzazione, che comporta la violazione di norme realizzando alcuni dei principali reati informatici regolamentati nell'attuale assetto normativo italiano. Il *cyberattack* si può differenziare a seconda del soggetto che lo commette, potrebbe essere un soggetto esterno rispetto alla realtà aziendale che riesce a prendere il controllo dei sistemi informatici dell'organizzazione, come se fosse localmente connesso alla macchina interna sotto attacco, anche se di fatto rimane distante centinaia o migliaia di chilometri[224]. Viceversa, ciò che interessa qualora si analizzi il D. Lgs. 231/2001, l'attore malevolo responsabile dell'attacco è un soggetto interno all'organizzazione, si parla del c.d. *Insider Threat*[225]. Per contrastarli l'azienda deve adottare una serie di contromisure tecniche e procedurali per realizzare un sistema più sicuro e deve dimostrare di aver fatto il possibile per prevenire tali attacchi, in modo da non risultare responsabile di dette violazioni.

Come analizzato nel precedente paragrafo ai fini dell'imputazione della responsabilità amministrativa da reato dell'ente come elemento costitutivo si prevede la commissione di un reato c.d. presupposto, perciò rientrante nel catalogo normativo contenuto nel D. Lgs. 231/2001.

Per quanto attiene ai reati informatici, di fondamentale importanza è stata la legge dell'8 maro 2008, n. 48 che ha introdotto nel D. Lgs. 231/2001 l'art. 24-*bis* rubricato "Delitti informatici e trattamento illecito di dati"; grazie a questo articolo l'ente potrà essere responsabile anche nel caso in cui un soggetto apicale o sottoposto commetta un reato informatico tra quelli previsti.

---

[224] cit. L. LUPARIA [et. al.], A. MONTI (a cura di), op. cit., p. 2.

[225] Secondo il report internazionale ENISA *Threat Landscape* 2020, *Insider Threat* il costo medio annuale sostenuto da una singola organizzazione per riparare i danni causati da attacchi di tipo *insider* è di oltre 11.45 milioni di euro. Come esempio vd. D. FIORONI, *Attacco Hacker a Leonardo Spa, 2 arresti*, in *poliziadistato.it*, 5 dicembre 2020.

Le attività nelle quali detti reati possono essere commessi sono proprie di ogni ambito aziendale che utilizza tecnologie dell'informazione. I reati informatici hanno come presupposto la disponibilità di un terminale[226] e la concreta disponibilità di accesso alle postazioni di lavoro; per tale ragione le aree di attività ritenute più a rischio, c.d. aree di attività a rischio[227], sono quelle che comportano l'utilizzo di un *personal computer*, l'accesso alla posta elettronica, l'utilizzo di programmi informatici e l'accesso ad *Internet*.

L'obbiettivo auspicato con suddetto intervento normativo era di comminare sanzioni penali alle persone fisiche e sanzioni "amministrative" alle persone giuridiche anche nel caso di reati informatici, vista la loro diffusività e pericolosità[228].

L'art. 24-*bis* del D. Lgs. 231/2001 prevede: «1. *In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.* 2. *In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.* 3. *In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, e dei delitti di cui all'articolo 1, comma 11, del decreto-legge 21 settembre 2019, n. 105, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.* 4. *Nei casi di condanna*

[226] Il "terminale" è una parte fondamentale di ogni sistema operativo, esso, infatti, è il dispositivo principale attraverso il quale possiamo inserire dati in un *computer* o in un sistema di elaborazione.

[227] In un'azienda vige il principio di "*risk assessment*", per cui si devono identificare e valutare i rischi inerenti al verificarsi di situazioni problematiche, in un'ottica di "*risk management*", per cui il governo dell'azienda dev'essere in grado di gestire tali rischi. Per "aree di attività a rischio" ci si riferisce alle aree o settori di attività aziendale nelle quali si potrebbero astrattamente verificare eventi pregiudizievoli, come reati.

[228] Come imposto dalle fonti sovranazionali, in particolare, dalla Convenzione *Cybercrime* del 2001 all'art. 12 rubricato "responsabilità delle persone giuridiche" ; dall'art. 8 della decisione quadro del Consiglio dell'Unione europea 2005/222/GAI, poi sostituita dalla direttiva del Parlamento europeo e del Consiglio 2013/40/UE relativa agli attacchi contro i sistemi di informazione, il cui art. 10 stabilisce parimenti l'obbligo di introdurre, per i reati informatici, la responsabilità amministrativa da reato delle persone giuridiche, pur lasciando la libertà agli Stati membri di stabilire la natura delle sanzioni da applicare, che possono essere anche di natura amministrativa e non strettamente penale, come accade in Italia (cit. L. LUPARIA [et. al.], A. MONTI (a cura di), op. cit., pp. 23 e 24).

*per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)*». Si può da subito notare come l'articolo non esaurisca il novero dei reati informatici esistenti, ma si limiti a disciplinare i "reati informatici in senso stretto"[229]; proprio per questo motivo viene criticato perché non in grado di realizzare un'organica e compiuta estensione della responsabilità da reato dell'ente nel caso di commissione di reati cibernetici.

Fondamentale, per il corretto inquadramento delle fattispecie di reato contemplate dall'art. 24-*bis* è la definizione di "sistema informatico", ovvero ogni sistema di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione di tecnologie informatiche, che sono caratterizzate dalla registrazione o memorizzazione di dati su supporti adeguati, per mezzo di impulsi elettronici.

L'art. 24-*bis* richiama chiaramente il "trattamento illecito di dati personali", ancorché, poi, l'elencazione in esso contenuta non citi nessuna delle fattispecie di cui agli artt. 167 e ss. del Codice della *privacy*[230] novellato. Inizialmente, il decreto legge n. 93/2013 aveva disposto l'inserimento delle fattispecie incriminatrici del Codice della *privacy* all'interno del novero dei reati presupposto. Tuttavia, in sede di conversione di detto decreto legge, il riferimento esplicito ai reati in materia di *privacy* è venuto meno; questo, probabilmente, per limitare l'impatto che tale nuova normativa avrebbe avuto sugli enti, anche in considerazione della mole di dati gestiti e della quantità di attività di trattamento da essi svolte[231]. A tal proposito, la relazione della Corte di Cassazione n. III/01/2013, commenta affermando come il richiamo ai delitti previsti dal Codice della *privacy* sia: «*di grande impatto, soprattutto per la configurazione della responsabilità da reato degli enti per l'illecito trattamento dei dati, violazione potenzialmente in grado di*

[229] vd. par. 1.2.1.
[230] Ci si riferisce sempre al D. Lgs. 196/2003.
[231] cit. P. BALBONI, F. TUGNOLI, op. cit., p. 3.

*interessare l'intera platea delle società commerciali e delle associazioni private soggette alle disposizioni del D. Lgs. 231/2001*».

Rimane comunque nella rubrica della norma il richiamo al trattamento illecito di dati personali, probabilmente perché, inevitabilmente, nel caso di commissione di illeciti informatici, si intersecano profili di interdisciplinarità con il trattamento illecito di dati. Qualora si verifichi una qualsiasi delle fattispecie incriminatrici previste all'art. 24-*bis*, di conseguenza si verificherà anche un illecito trattamento di dati personali, tant'è che la società, sia essa responsabile o titolare del trattamento, dovrà avviare delle indagini interne atte a verificare se vi sia stata una compromissione dei dati trattati ed eventualmente aprire una procedura per la gestione dei casi di violazione ai sensi degli artt. 33 e 34 del GDPR. In ogni caso, è auspicabile un intervento legislativo di ampio respiro che disciplini la responsabilità amministrativa da reato degli enti nel caso di violazioni penali *privacy* ai sensi degli art. 167 e ss. del Codice *privacy*.

### 3.3.1. *Il trattamento illecito di dati* ex *art. 167 Codice della* privacy

Appare doverosa una disamina del trattamento illecito di dati *ex* art. 167 Codice della *privacy*, il quale statuisce: «1. *Salvo che il fatto non costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno, operando il violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129, arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi.* 2. *Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2-septies arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni*. 3. *Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati*

*personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.* 4. *Il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante.* 5. *Il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attività di accertamento delle violazioni delle disposizioni di cui al presente decreto.* 6. *Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita*».

Si tratta di una norma penale in bianco, ragion per cui non contiene una descrizione completa delle condotte vietate, ma rinvia ad altre norme contenute nel Codice della *privacy* che stabiliscono i criteri di liceità di un trattamento di dati, ovvero a disposizioni di rango secondario e di futura emanazione o in provvedimenti generali del Garante, incidendo negativamente sulla tassatività e determinatezza della fattispecie. Inoltre, l'articolo esordisce con una clausola di riserva espressa, anche questo contribuisce alla sua poca chiarezza ed immediatezza.

Guardando al bene giuridico tutelato si nota come la disposizione non protegge semplicemente la riservatezza dei dati personali dalle turbative provocate dai terzi, ma anche l'eventuale pregiudizio all'onore e alla reputazione subito dalla persona offesa, potendo in ogni caso la condotta arrecare lesioni alla sfera più intima della riservatezza e dell'autodeterminazione. Per quanto riguarda l'elemento soggettivo si richiede un dolo specifico che restringe notevolmente l'area applicativa.

Si sono da sempre delineate opinioni discordanti sulla nozione di "nocumento", ci si interroga se sia corretto qualificarlo come elemento costitutivo ovvero come condizione obbiettiva di punibilità.

La precedente giurisprudenza interpretava il nocumento come condizione

obbiettiva di punibilità, ossia come elemento esterno alla fattispecie, di per sé già perfetta in termini di rispondenza all'ipotesi astratta delineata dal legislatore, che tuttavia risulta punibile solo se ricorre un danno effettivo per l'interessato[232].

Vi è stato un cambiamento nell'impostazione giurisprudenziale per cui il nocumento viene interpretato come elemento costitutivo, solo in questo modo si può adeguare la fattispecie incriminatrice al principio di colpevolezza *ex* art. 27 Cost. Sul punto, fondamentale, la sentenza della Corte di Cassazione, sez. III, n. 40103 del 5 febbraio 2015, la quale recita: «*In tema di trattamento illecito dei dati personali, il nocumento per la persona alla quale i dati illecitamente trattati si riferiscono, previsto dall'art. 167 del D. Lgs. 30 giugno 2003, n. 196, costituisce, per la sua omogeneità rispetto all'interesse leso, e la sua diretta derivazione causale dalla condotta tipica, un elemento costitutivo del reato, e non una condizione oggettiva di punibilità; ne consegue che esso deve essere previsto e voluto o comunque accettato dall'agente come conseguenza della propria azione, indipendentemente dal fatto che costituisca o si identifichi con il fine dell'azione stessa*». Tale nuova interpretazione ha ricadute sia sulla sussistenza in sé della rilevanza penale della condotta, poiché in difetto di nocumento manca il reato, sia sull'elemento soggettivo, in quanto il dolo, dovendo investire tutto il fatto tipico, ora deve abbracciare anche il nocumento[233].

L'orientamento preferibile propende per qualificare il nocumento come condizione obbiettiva di punibilità; per cui, si ha un'imputazione oggettiva delle condotte a prescindere dalla volontà di ledere il bene giuridico *privacy* perché le condotte sono ritenute "bisognose di pena". Il nocumento funge da "valvola" per evitare un eccessivo ampliamento ovvero un eccessivo restringimento della fattispecie, alcune condotte non vengono punite perché al di sotto di questa "soglia" non hanno bisogno di una pena e lo Stato può disinteressarsi.

---

[232] vd. Cass. pen., sez III, n. 7504 del 16 luglio 2013, sent. secondo la quale: «*Il nocumento, previsto dall'*art. *167 d.lg. n. 196 del 2003 quale condizione obiettiva di punibilità del reato di trattamento illecito di dati personali, non è soltanto quello derivato alla persona fisica o giuridica cui si riferiscono i dati, ma anche quello causato a soggetti terzi quale conseguenza dell'illecito trattamento (nella specie, i congiunti di minore vittima di incidente stradale, la cui fotografia, unitamente ad altri dati identificativi, era stata pubblicata a mezzo stampa*».

[233] cit. P. BALBONI, F. TUGNOLI, op. cit., p. 7.

I commi 4 e 5 dell'articolo in esame prevendono una serie di modalità di collaborazione tra il Garante e il Pubblico Ministero nei casi di notizia delle già menzionate ipotesi di reato, si devono informare senza ritardo a vicenda. Entrambe dette Autorità dovrebbero modulare le rispettive sanzioni, conformemente a quanto previsto al Considerando n. 149 del GDPR[234] e nel rispetto del *ne bis in idem*, prevedendo una diminuzione della sanzione penale nel caso in cui sia già stata riscossa la sanzione amministrativa.

### 3.3.2. *Conclusioni*

In conclusione, si vede come i reati informatici la cui commissione comporta la responsabilità delle persone giuridiche, previsti nel D. Lgs. 231/2001, non appaiono sufficienti a contrastare la criminalità informatica e cibernetica. Non si può restringere l'attenzione ai soli delitti previsti all'art. 24-*bis*, ma occorre un approccio generale, con l'obbiettivo di combattere la criminalità commessa nel *Cyberspace*, in ogni sua sfaccettatura.

Inoltre, non è sempre agevole l'accertamento della responsabilità dell'ente, vi è una complessità che nasce, da un lato, dall' immaterialità e tendenza alla dissolvenza delle informazioni e dei dati gestiti per mezzo di strumenti informatici e telematici; dall'altro lato, dall'inadeguatezza del linguaggio giuridico, soprattutto di quello penalistico, nel descrivere le caratteristiche della condotta e del fatto e la constante proliferazione delle modalità di aggressione ai sistemi informatici[235].

---

[234] *Ex* Considerando n. 149 del GDPR: «*Gli Stati membri dovrebbero poter stabilire disposizioni relative a sanzioni penali per violazioni del presente regolamento, comprese violazioni di norme nazionali adottate in virtù ed entro i limiti del presente regolamento. Tali sanzioni penali possono altresì autorizzare la sottrazione dei profitti ottenuti attraverso violazioni del presente regolamento. Tuttavia, l'imposizione di sanzioni penali per violazioni di tali norme nazionali e di sanzioni amministrative non dovrebbe essere in contrasto con il principio del ne bis in idem quale interpretato dalla Corte di giustizia*».

[235] cit. A. CADOPPI [et. al.], op. cit., p. 204.

## 3.4. *Clausole di esonero della responsabilità dell'ente: i Modelli organizzativi nel dettaglio*

### 3.4.1. *Il Modello 231*

Nel precedente paragrafo si è già avuto modo di accennare alle clausole di esonero della responsabilità dell'ente nel caso in cui predisponga dei c.d. Modelli Organizzativi 231[236].

L'ente, affinché possa applicarsi la clausola di esonero, deve provare che le persone fisiche, nella commissione dell'illecito penale, abbiano eluso fraudolentemente i Modelli di gestione ed organizzazione e che non vi è stata o vi sia stata un'insufficiente vigilanza da parte dell'Organismo di vigilanza.

Per quanto attiene al caso di commissione di un illecito, tra quelli previsti, da parte di un soggetto apicale, l'ente potrà essere esente da responsabilità se prova la sussistenza della serie di requisiti concorrenti descritti all'art. 6, comma 1[237].

Detti Modelli di organizzazione e gestione devono contenere: l'individuazione delle aree sensibili nelle quali potrebbero commettersi reati e il grado di "rischiosità", c.d. *risk assessment*; la previsione di specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente, in relazione ai reati da prevenire; la specificazione delle modalità di gestione delle risorse finanziarie utilizzate per impedire la commissione di illeciti; la previsione di obblighi di informazione nei confronti dell'Organismo deputato a vigilare sul funzionamento e sul rispetto del MOG, c.d. flussi informativi; l'introduzione

[236] Ci si riferisce ai Modelli di organizzazione, gestione e controllo (MOGC); anche detti, in inglese: *compliance programs*.

[237] *Ex* art. 6, comma 1 del D. Lgs. 231/2001: «*Se il reato è stato commesso dalle persone indicate nell'articolo 5, comma 1, lettera a), l'ente non risponde se prova che: a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi; b) il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo; c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione; d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b)*».

di un sistema disciplinare per sanzionare il mancato rispetto delle misure indicate nel Modello[238].

L'obbiettivo auspicato consiste nel realizzare un sistema di controllo in grado di prevenire i rischi, che si potrà raggiungere seguendo un processo di c.d. *risk management*[239]. Analizzando brevemente le tappe principali di detto processo troviamo, prima di tutto, l'identificazione dei rischi potenziali: ossia l'analisi del contesto aziendale per individuare quali sono le aree sensibili di attività e secondo quali modalità si potrebbero astrattamente verificare eventi pregiudizievoli per gli obiettivi indicati dal Decreto 231. Per "rischio" si intende qualsiasi variabile o fattore che nell'ambito dell'azienda, da solo o in correlazione con altre variabili, possa incidere negativamente sul raggiungimento degli obiettivi indicati dal Decreto, in particolare, all'art. 6, comma 1, lett. a); pertanto, a seconda della tipologia di reato, gli ambiti di attività a rischio potranno essere più o meno estesi. Si passa poi alla progettazione del sistema di controllo, c.d. "protocolli" per la programmazione della formazione e attuazione delle decisioni dell'ente, ossia la valutazione del sistema esistente all'interno dell'ente per la prevenzione dei reati ed il suo eventuale adeguamento, in termini di capacità nel contrastare efficacemente, cioè ridurre ad un livello accettabile, i rischi identificati.

Nella progettazione dei sistemi di controllo preventivo a tutela dei rischi è fondamentale il concetto di rischio accettabile[240], è necessario identificare una soglia effettiva che ponga un limite alla quantità e qualità delle misure di prevenzione da introdurre per evitare la commissione di reati. Nei reati dolosi la soglia di accettabilità è rappresentata da un sistema di prevenzione tale da non poter essere aggirato se non fraudolentemente; mentre, per quanto attiene ai reati colposi la soglia è rappresentata dalla realizzazione di una condotta in violazione del modello organizzativo di prevenzione[241].

---

[238] *Ex* art. 6, comma 2 del D. Lgs. 231/2001.

[239] L'UNI 11230, Vocabolario nazionale, Gestione del Rischio, lo definisce come: «*l'insieme di attività, metodologie e risorse coordinate per guidare e tenere sotto controllo un'organizzazione con riferimento ai rischi*».

[240] Concettualmente il rischio è ritenuto accettabile quando i controlli aggiuntivi "costano" di più della risorsa da proteggere.

[241] cit. CONFINDUSTRIA, *Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo, ai sensi del decreto legislativo 8 giugno 2001, n. 231*, 2021, pp. 39 e 40.

Il comma 2-*ter* dell'art. 6 del D. Lgs. 231/2001 disciplina il sistema di segnalazioni, strumento attraverso il quale si da la possibilità a tutti i soggetti coinvolti all'interno dell'ente di formulare segnalazioni relativamente ad eventuali violazioni del MOG di cui vengono a conoscenza. Infine, il comma 3 del medesimo articolo chiarisce che i MOG possono essere adottati sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti, i quali non sono cogenti, ma fungono da linee guida.

Il MOG dev'essere adottato prima della commissione del reato, dev'essere idoneo a prevenire i reati della specie di quello realizzatosi e dev'essere attuato efficacemente.

Il giudizio circa l'idoneità, la concreta implementazione e l'efficace attuazione del Modello, nella quotidiana attività dell'impresa, è rimesso alla libera valutazione del giudice. È di fondamentale importanza, affinché al modello sia riconosciuta efficacia esimente, che l'impresa compia una seria e concreta opera di implementazione delle misure adottate nel proprio contesto organizzativo. Il Modello non deve rappresentare un mero adempimento burocratico, esso deve vivere nell'impresa, aderire alle caratteristiche della sua organizzazione, evolversi e cambiare con essa[242].

Per quanto attiene ai soggetti sottoposti l'art. 7, comma 2 del D. Lgs. 231/2001 prevede una clausola di esonero dalla responsabilità dell'ente qualora abbia efficacemente attuato un MOG idoneo a prevenire i reati della specie di quello commesso. Le caratteristiche di suddetto MOG sono disciplinate al comma 3 del medesimo articolo, che recita: «*Il modello prevede, in relazione alla natura e alla dimensione dell'organizzazione nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio*», mentre ai fini di un'efficace attuazione del MOG il comma 4 prevede: «*a) una verifica periodica e l'eventuale modifica dello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività; b) un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello*». Per quanto riguarda le modifiche da apportare

[242] cit. CONFINDUSTRIA, op. cit., p. 4.

necessariamente al MOG, basti pensare a quando, nel 2020 con il D. Lgs. n.75[243] sono stati inseriti, all'interno del catalogo dei reati presupposto, i reati tributari; a seguito di tale cambiamento normativo tutti i Modelli di gestione ed organizzazione, prima di allora adottati, dovettero essere necessariamente modificati affinché potessero prevedere una mappatura dei rischi inerenti all'area sensibile nella quale i reati tributari potevano verificarsi.

Riassumendo, Il Modello 231 si articola come segue: parte generale che rappresenta un documento di sintesi del complesso organico di regole di buon governo societario funzionali alla gestione ottimale del rischio reato il cui obbiettivo è quello di fornire ai destinatari un quadro sulla realtà aziendale[244]; parte speciale, afferente alle diverse tipologie di reati presupposto contemplate nel Decreto 231, e recante la mappatura dei rischi di commissione di detti reati; codice etico, contenente le regole di condotta proprie dell'organizzazione; sistema disciplinare, riportante le regole sanzionatorie; flussi informativi rivolti all'Organismo di Vigilanza; regolamento dell'Organismo di Vigilanza; sistema di procure e deleghe; organizzazione gerarchico-funzionale. Tuttavia, bisogna ricordare che il Modello 231 nel suo insieme dovrà necessariamente essere costruito in base alle esigenze e alle caratteristiche specifiche di ogni singolo ente.

#### 3.4.1.1. *Il MOGC idoneo a prevenire la commissione di reati informatici*

Il Modello organizzativo adottato da un'azienda ha l'obbiettivo di prevenire e dissuadere la realizzazione di reati presupposto, tra i quali vi rientrano anche i reati informatici, rispetto ai quali la possibilità di commetterli aumenta esponenzialmente stante l'evoluzione incessante delle tecnologie e dei dispositivi in uso. In seguito, verrà

[243] Il decreto legislativo n. 75 del 14 luglio 2020 ha recepito la direttiva UE n. 2017/1371, c.d. direttiva P.I.F. (Protezione Interessi Finanziari), recante norme per "la lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale".

[244] cit. G. URICCHIO, *Modello Privacy e Modello Organizzativo. Approcci e similitudini tra la disciplina relativa al trattamento dei dati personali ai sensi del Regolamento UE 2016/679 e la disciplina del D. Lgs. 231/2001*, in *Altalex*, 2021, p. 2.

analizzato nel dettaglio il Modello di organizzazione e gestione ritenuto efficace e idoneo a prevenire i reati informatici. È essenziale che un'azienda adotti specifici protocolli e presidi di gestione integrati e interconnessi tra le diverse aree di *compliance*[245].

Per quanto attiene al MOG idoneo ad evitare la commissione di delitti informatici, si predispone una sezione speciale *ad hoc*, c.d. parte speciale, nella quale si indicano le misure adottate al fine di scongiurare il verificarsi di comportamenti illeciti connessi alla disponibilità di mezzi informatici, in quanto la sicurezza dei sistemi informatici è ritenuta un elemento essenziale del sistema di controllo aziendale e in ragione del fatto che il sistema informatico prevede la gestione di tutti i dati aziendali, occorre pertanto un corretto utilizzo dello stesso.

In questa parte speciale, prima di tutto si andranno a delineare le fattispecie di reato per le quali l'art. 24-*bis* del D. Lgs. 231/2001 prevede una responsabilità degli enti, nei casi in cui tali reati siano stati compiuti nell'interesse o a vantaggio degli stessi. In seguito, si provvede all'individuazione delle attività a rischio, le quali si potrebbero ravvisare nella: gestione ed utilizzo dei sistemi informatici e delle informazioni aziendali, il c.d. patrimonio informativo, nell'ambito del quale possono essere ricomprese diverse attività (gestione del profilo utente e del processo di autenticazione, gestione e protezione della postazione di lavoro ecc.); e nella gestione delle autorizzazioni e delle licenze di programmi *software* e banche dati. La società deve poi predisporre procedure specifiche con appositi presidi organizzativi, cercando adeguate soluzioni di sicurezza da tenere sempre in aggiornamento, come la previsione di *password* ovvero codici di accesso riservati nominativi o numerici. Si individuano una serie di principi generali di comportamento per cui si predispone l'espresso divieto a carico dei destinatari di porre in essere, o concorrere in qualsiasi forma nella realizzazione, di comportamenti tali da

[245] La funzione "*compliance*" effettua i controlli sulla conformità alle disposizioni di legge, ai provvedimenti delle Autorità di Vigilanza e alle norme di autoregolamentazione nonché a qualsiasi norma applicabile. Devono essere valutati i rischi di non conformità alle norme, per evitare di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni di reputazione in conseguenza di violazione di norme imperative (leggi, regolamenti) ovvero di autoregolamentazione (statuti, procedure interne, codice di autodisciplina). La funzione *compliance*, con riferimento al Modello adottato 231, ha tra i suoi compiti sia quello di valutare la corretta conformità normativa sia quello di salvaguardare la società dal rischio di non conformità con riferimento ai danni reputazionali (cit. F. BIANCHI, *La funzione compliance e il Modello 231*, in *Rivista 231*, 2010).

integrare le fattispecie di reato considerate. Si delinea il sistema di controllo nel quale opera l'Organismo di Vigilanza, che effettua periodicamente specifici controlli sulle attività potenzialmente a rischio, al fine di verificare il rispetto dei principi generali di comportamento, delle procedure e delle istruzioni operative.

Come prima accennato un ente si deve proteggere dagli attori malevoli appartenenti all'organizzazione[246], che alterano intenzionalmente i programmi, la logica o i dati del sistema informatico aziendale al fine di commettere crimini informatici[247], proprio perché sono *insider* riescono a commettere detti illeciti con maggiore facilità avendo piena conoscenza dei meccanismi di sicurezza e avendo la possibilità di coprire le loro tracce. Per tutelarsi l'azienda dovrà predisporre un sistema sicuro di registrazione degli eventi che accadono nel sistema informatico aziendale, c.d. *logging*[248] sicuro, in modo tale da poter dimostrare di aver fatto il possibile per prevenire la commissione di reati informatici[249].

Un *logging* sicuro da solo non basta a garantire un adeguato livello di sicurezza, è necessaria una *governance*[250] efficace dei processi e delle risorse del sistema aziendale che si realizza attraverso una separazione dei ruoli, per cui attraverso un sistema di monitoraggio dei dipendenti si individuano eventuali comportamenti anomali.

Nella redazione dei Modelli 231 occorrerà verificare il grado di sviluppo tecnologico dell'ente, che in un'ottica di *risk oriented*[251], consentirà di individuare i presidi di sicurezza per la struttura aziendale; si deve calcolare il rischio di commissione di condotte illecite sulla base della possibilità che l'evento si verifichi relativamente ad una determinata area sensibile di attività dell'azienda.

---

[246] Il rischio da prevenire con il Modello 231 è quello relativo alla commissione di illeciti commessi da un soggetto interno all'ente, a vantaggio o nell'interesse dell'ente; mentre, per quanto attiene agli attacchi subiti da soggetti estranei rispetto all'ente, che costituiscono *ipso iure* un rischio alla *privacy*, l'ente non potrà incorrere in alcuna responsabilità.

[247] cit. L. LUPARIA [et. al.], A. MONTI (a cura di), op. cit., p. 3.

[248] In italiano: "registrazione".

[249] La comunità scientifica ha progettato e sviluppato diversi protocolli in materia di *logging* sicuro, per esempio vd. B. SCHNEIER, J. KELSEY, *Cryptographic support for secure logs on un-trusted machines*, in *The 7th USENIX Security Symposium Proceedings*, USENIX Press, January 1998, 53-62.

[250] Per "*governance*" si intende l'insieme dei principi, delle regole e delle procedure che riguardano la gestione e il governo di una società, di un'istituzione, di un fenomeno collettivo.

[251] In italiano: "orientata al rischio".

L'obbiettivo principale per l'ente, nel perseguimento della finalità di sicurezza informatica è di garantire i seguenti principi: suddivisione dei profili autorizzativi nel rispetto del principio di *least privilege*[252]; riservatezza delle informazioni; integrità del dato aziendale; tracciabilità e sicurezza delle informazioni che vengono trattate, in modo tale da non essere manomesse o modificate da soggetti non autorizzati; disponibilità dei dati in funzione delle esigenze e nel rispetto delle norme che ne impongono la conservazione. Detti obbiettivi si possono perseguire attraverso protocolli comportamentali che prevedono obblighi e/o divieti specifici per ogni tipologia di reato[253].

Ai fini di una mitigazione dei reati informatici si adottano elevati standard di sicurezza, come quelli previsti dalle certificazioni internazionali quali la ISO/IEC 27001:2022[254]; tenendo a mente, che: «*nessun sistema è del tutto sicuro, esiste un livello accettabile di sicurezza che è definito dal bilanciamento di varie componenti, come il valore di quanto si intende difendere, l'investimento economico che si è disposti a sostenere, il livello di rischio che si è disposti a tollerare. È quindi necessario addivenire ad un ragionevole compromesso tra tutte le esigenze in gioco*»[255].

Un ulteriore elemento di mitigazione concerne il rispetto del Provvedimento del Garante *privacy*, "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", del 27 novembre 2008, che riguarda la nomina e i requisiti degli Amministratori di Sistema, c.d. AdS[256].

---

[252] Adottare il principio *least privilege* significa che ogni utente, programma, processo o dispositivo connesso abbia solo i privilegi minimi necessari per eseguire la sua mansione o la sua funzione; cosicché si possa definire una strategia di sicurezza che mira a mitigare il rischio di violazione dei dati aziendali (cit. E. FILADELFIO, *Least privilege: dati al sicuro da accessi non autorizzati col principio del privilegio minimo*, in *cybersecurity360.it*, 2021).

[253] cit. P. BALBONI, F. TUGNOLI, op. cit., p.12.

[254] ISO/IEC 27001 è uno standard sulla sicurezza informatica che definisce i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni (SGSI o ISMS, dall'inglese *Information Security Management System*) ed include aspetti relativi alla sicurezza logica, fisica ed organizzativa.

[255] cit. G. VACIAGO, *Compliance 231. Modelli organizzativi e OdV tra prassi applicative ed esperienze di settore*, Gruppo Sole 24 Ore, Milano, 2020, p. 196.

[256] Gli "amministratori di sistema" sono figure essenziali per la sicurezza delle banche dati e la corretta gestione delle reti telematiche. Sono esperti chiamati a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali. Ad essi viene

### 3.4.2. *L'Organismo di Vigilanza*

Contestualmente all'adozione del Modello 231[257], l'ente nomina un Organismo di Vigilanza, anche detto OdV, dotato di autonomi poteri di vigilanza, iniziativa e controllo. Tale organo riveste un ruolo essenziale, in quanto l'esenzione della responsabilità dell'ente dipende dalla capacità dell'OdV a garantire l'efficienza e l'operatività del MOG, attraverso attività di controllo sull'idoneità di esso a prevenire la commissione di reati presupposto e sulla sua effettività all'interno dell'ente.

In ragione della complessità dell'azione di controllo gravante sull'OdV si ritiene opportuno stilare una schematica ricostruzione dei tre momenti principali in cui essa si suddivide: redazione del piano delle attività, modalità di verifica e valutazione sull'esito[258]. Inoltre, è obbligato ad aggiornare i Modelli, garantendone una stabilità e funzionalità, proponendo eventuali modifiche all'organo dirigente competente ad apportale.

Come ogni componente del Modello, anche detta istituzione deve essere guidata dal principio di effettività, ossia non deve rappresentare un adempimento meramente formale; l'Organismo dev'essere posto nelle condizioni di assolvere realmente ai complessi e delicati compiti di cui la legge lo investe.

L'OdV deve caratterizzarsi per quattro requisiti elaborati dalla giurisprudenza: indipendenza, autonomia, assenza di conflitto d'interessi e continuità di azione.

L'Organismo deve agire libero da ogni forma di interferenza e condizionamento da parte di tutti gli organi dell'ente, evitando situazioni di conflitto di interessi, anche potenziale, con il vertice, che potrebbero configurarsi, ad esempio, nell'ipotesi di attribuzione di compiti operativi[259].

---

affidato spesso anche il compito di vigilare sul corretto utilizzo dei sistemi informatici di un'azienda o di una pubblica amministrazione (cit. *Amministratori di sistema: occorre massima trasparenza sul loro operato. Il Garante fissa i criteri, quattro mesi per mettersi in regola*, 2008, in *garanteprivacy.it*).

[257] Ci si riferisce sempre al modello di organizzazione e gestione, c.d. MOG ovvero, introducendo anche il concetto di controllo, MOGC.

[258] cit. L. FRUSCIONE, A. GIUSTINI, *Gli aspetti organizzativi dell'attività di controllo del Modello 231*, in *Rivista 231*, 2019, abstract.

[259] vd. Trib. Torino, 14 novembre 2011, Seconda Corte di Assise; Corte di Assise di Appello di Torino, 28 febbraio 2013; Cass. pen., sez. V, 30 gennaio 2014, n. 4677.

Il requisito di autonomia prevede che la posizione dell'OdV debba essere caratterizzata da un'autonomia nell'iniziativa di controllo. Inoltre, la giurisprudenza ha affiancato al requisito dell'autonomia quello dell'indipendenza[260]. Il primo requisito, infatti, sarebbe svuotato di significato se i membri dell'Organismo di Vigilanza risultassero condizionati a livello economico e personale o versassero in situazioni di conflitto di interesse, anche potenziale. Dev'essere sufficientemente indipendente dall'ente in modo tale da riuscire a valutare il Modello, individuarne le eventuali violazioni ed intervenire.

Per quanto attiene al requisito di continuità dell'azione esso potrà essere rispettato attraverso la predisposizione di una struttura dedicata all'attività di vigilanza, con la cura della tracciabilità e della conservazione inerente alla documentazione delle attività svolta da parte dello stesso Organismo.

L'OdV affinché possa svolgere efficacemente la propria attività deve possedere le competenze in «*attività ispettiva, consulenziale, ovvero la conoscenza di tecniche specifiche, idonee a garantire l'efficacia dei poteri di controllo e del potere propositivo ad esso demandati*»[261]; è inoltre preferito che almeno qualche membro dell'Organismo abbia competenze in tema di analisi dei sistemi di controllo e competenze di tipo giuridico, in particolare, in ambito penalistico.

Inoltre, sempre la giurisprudenza con il l'ordinanza del 4 aprile 2003 G.i.p., del Tribunale di Roma, ha statuito: «*al fine di garantire efficienza e funzionalità l'organismo di controllo non dovrà avere compiti operativi che, facendolo partecipe di decisioni dell'attività dell'ente, potrebbero pregiudicare la serenità di giudizio al momento delle verifiche*».

La legge non prevede le concrete modalità di funzionamento dell'Organismo di Vigilanza, queste si sono stabilite in via di prassi attraverso una serie di regole di "buona condotta". La legge statuisce unicamente che, affinché l'ente possa essere esente da

[260] cfr. Trib. Milano, G.i.p., 09 novembre 2004, *Esame dell'idoneità dei modelli di organizzazione, gestione e controllo ex artt 6 e 7 d.lg. 231/2001,* ord.

[261] cit. Trib. Napoli, G.i.p., 26 giugno 2007, *Idoneità del Modello di organizzazione e gestione per la prevenzione dei reati presupposto*, ord.

responsabilità, l'OdV dev'essere presente e deve adempiere sufficientemente all'obbligo di vigilanza[262].

La dottrina si è a lungo interrogata sulla composizione dell'organo, dato che la legge nulla dispone al riguardo, si ritiene opportuno attribuire dette funzione ad organi già esistenti all'interno dell'assetto societario e dotati di poteri di controllo, quali il collegio sindacale, l'*internal audit*[263], il comitato di controllo interno, ovvero ad una struttura *ad hoc*, composta da soggetti caratterizzati da professionalità ed indipendenza, portatori di interessi differenti, interni ed esterni alla compagine sociale[264]. Si prediligono organismi collegiali in grado di assicurare una maggiore diversificazione delle competenze sulle varie tipologie di reati ed una maggiore indipendenza dell'organo. Il comma 4 dell'art. 6 prevede un'eccezione per la quale, nel caso di enti di piccole dimensioni, i compiti di controllo possano essere svolti direttamente dall'organo dirigente; si tratta di un'eccezione finalizzata ad un risparmio di costi e adattata alle dimensioni dell'ente, normalmente l'OdV non può mai coincidere con la direzione interna, altrimenti controllore e controllato si sovrapporrebbero[265].

Il comma 4-*bis* dell'art. 6 ha chiarito ogni dubbio circa la compatibilità del ruolo

---

[262] Il concetto di adempiere "sufficientemente" all'obbligo di vigilanza è stato elaborato nel tempo dalla prassi, pur non essendo prevista una cadenza sui controlli e sulle riunioni, anche perché non potrebbe sussistere una regola universale in tal senso dato che l'attività dell'OdV dev'essere adeguata al tipo e alle dimensioni dell'ente in cui opera.

[263] La definizione di "attività di *internal audit*" fornita dall'AIIA (Associazione Italiana *Internal Auditors*) chiarisce che l'*Internal Auditing* costituisce un'attività indipendente ed obiettiva di *assurance* e consulenza, finalizzata al miglioramento dell'efficacia e dell'efficienza dell'organizzazione. Assiste l'organizzazione nel perseguimento dei propri obiettivi tramite un approccio professionale sistematico, che genera valore aggiunto in quanto finalizzato a valutare e migliorare i processi di controllo, di gestione dei rischi e di *corporate governance*.

[264] cit. E. M. AMBROSETTI [et. al.], op. cit., p. 69.

[265] Ormai copiosa la giurisprudenza in merito, che ha stigmatizzato come inefficace il Modello che attribuisca, ad esempio, al dirigente del settore ecologia, ambiente e sicurezza il ruolo di membro dell'Organismo di vigilanza, deputato a vigilare efficacemente sull'adozione delle misure organizzative volte a prevenire infortuni sul lavoro: il fatto che il soggetto operi in settori oggetto delle attività di controllo dell'OdV esclude qualsiasi autonomia di quest'ultimo; il soggetto sarebbe chiamato a essere "giudice di se stesso", per di più dotato di poteri disciplinari, (cit. Corte di Assise di Appello di Torino, 22 maggio 2013, c.d. sent. *Thyssenkrupp*); o ancora laddove il Presidente dell'OdV, sia anche consigliere di amministrazione della società e il collegio integrato dal commercialista di fiducia della proprietà ed un soggetto apicale di una delle aziende del gruppo (cit. Cass. pen., sez. II, 9 dicembre 2016, n. 52316, sent., secondo cui iniziativa e controllo, possono essere ritenuti effettivi e non meramente "cartolari" soltanto ove risulti la non subordinazione del controllante al controllato).

svolto dai sindaci e quello proprio dei membri dell'Organismo di vigilanza, prevedendo esplicitamente che nelle società di capitali tali funzioni di controllo possano essere attribuite al collegio sindacale, al consiglio di sorveglianza o al comitato per il controllo sulla gestione[266].

Infine, la giurisprudenza sempre nell' ordinanza del 9 novembre 2004 del G.i.p. del Tribunale di Milano statuisce che: «*appare veramente eccessivo pretendere, perché operi la causa di ineleggibilità, che nei confronti del soggetto che si vorrebbe nominare quale componente dell'organo di vigilanza sia stata emessa sentenza di condanna divenuta irrevocabile*», poiché, anche prima della definitività della sentenza di condanna, il soggetto, pur se non colpevole sul piano penale, potrebbe non essere in una posizione di sufficiente indipendenza per rivestire il ruolo di membro dell'Organismo di vigilanza.

Resta ora da approfondire quanto previsto all'art. 6, comma 2, lett. d) del D. Lgs. 231/2001 in tema di obblighi di informazioni nei confronti dell'OdV. Secondo tale articolo sono predisposti una serie di flussi informativi, periodici e *ad hoc*, attraverso dei processi di comunicazione aziendali, aventi come destinatario l'Organismo affinché possa conoscere e gestire eventuali situazioni di rischio; così, agevolando la sua attività di vigilanza sull'efficacia del Modello e di accertamento a posteriori delle cause che hanno reso possibile il verificarsi di un reato. Analoga attività sarà compiuta dall'OdV, nei confronti dell'organo amministrativo e del collegio sindacale, in merito alle attività svolte, al funzionamento, all'aggiornamento ovvero alle eventuali criticità del Modello.

Va chiarito che le informazioni fornite all'Organismo di Vigilanza mirano a consentirgli di migliorare le proprie attività di pianificazione dei controlli e non, invece, ad imporgli un'attività di verifica puntuale e sistematica di tutti i fenomeni rappresentati. In altre parole, all'OdV non incombe un obbligo di agire, essendo rimesso alla sua discrezionalità, e responsabilità, lo stabilire in quali casi attivarsi[267].

---

[266] La dottrina e la giurisprudenza, prima dell'introduzione del comma 4-*bis* dell'art. 6 del D. Lgs. 231/2001, propendevano per sconsigliare all'ente di nominare nell'OdV un membro del collegio sindacale perché nei reati societari, considerati quali reati presupposto, i sindaci potevano essere soggetti attivi; quindi, l'OdV si trovava a vigilare su un suo stesso membro, con la conseguente identificazione tra controllore e controllato che viola il requisito di assenza del conflitto di interessi.

[267] cit. CONFINDUSTRIA, op. cit., p. 91.

L'OdV potrà ricevere segnalazioni di condotte illecite o di violazioni del Modello, come previsto agli artt. 2-*bis*, 2-*ter* e 2-*quater* del D. Lgs. 231/2001 inseriti con la Legge del 30 novembre 2017, n. 179 in materia di *whistleblowing*[268].

In conclusione, L'Organismo di Vigilanza potrebbe incorrere in una responsabilità penale nel caso di illeciti commessi in conseguenza al mancato esercizio del potere di vigilanza sull'attuazione e sul funzionamento del Modello 231. La fonte di detta responsabilità potrebbe rinvenirsi all'art. 40, comma 2 c.p. per cui «*non impedire un evento, che si ha l'obbligo giuridico di impedire, equivale a cagionarlo*»[269]; pertanto l'Organismo potrebbe essere punito a titolo di concorso omissivo nei reati commessi dall'ente. Ma, bisogna tenere a mente che l'obbligo di vigilanza che incombe su questo soggetto non comporta di per sé l'obbligo di impedire l'azione illecita, ovverosia l'Organismo non si trova in una posizione di garanzia rispetto al bene giuridico tutelato.

Non appare corretto attribuire a questo Organismo dei compiti che prevedono di impedire la commissione di reati, dato che formalmente non dispone di poteri impeditivi e ciò equivarrebbe ad attribuirgli doveri e compiti simili a quelli che, nel nostro ordinamento, ha la polizia giudiziaria.

---

[268] Legge del 30 novembre 2017, n. 179, recante "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato". Il termine "*whistleblowing*" di derivazione anglosassone, significa letteralmente "soffiare nel fischietto" e si riferisce a quello strumento legale ideato e collaudato negli Stati Uniti e in Gran Bretagna per garantire un'informazione tempestiva in merito ad eventuali tipologie di rischio, quali frodi ai danni o ad opera dell'organizzazione, negligenze, illeciti, minacce ecc.; lo si può quindi definire come la comunicazione da parte di uno o più membri di un'organizzazione lavorativa, di un'azione illegale, immorale o illegittima, posta in essere da un altro soggetto (cit. F. MARTINELLI, *Il fenomeno del whistleblowing*, in *Giurisprudenza penale web*, 2017, p. 4).

[269] L'articolo 40 del codice penale al comma 2 detta la particolare disciplina dei reati omissivi c.d. impropri. L'utilizzo del termine "equivale", presente nel dettato normativo, non ha valenza causale difatti la *voluntas legis* è chiara, equiparare la condotta omissiva a quella commissiva (si parla a tal proposito di "clausola di equivalenza"). Detta disposizione, di carattere estensivo, ha "aperto le porte" a nuove fattispecie commissive, concentrate sul mancato impedimento dell'evento dannoso, generando come necessaria conseguenza problemi di incompatibilità con i principi costituzionali, precisamente quelli di legalità e determinatezza. La dottrina, nel tentativo di ovviare ai problemi applicativi della norma *de quo*, ha indicato le ipotesi in cui è possibile ravvisare detta "equivalenza": nel caso di fattispecie commissive di evento e non anche per quelle di mera condotta, per i reati a forma libera, rilevando unicamente l'evento lesivo ed essendo irrilevanti le modalità con cui si è realizzato l'evento stesso (cit. T. J. MIRÒ D'ANIELLO, *L'*art. *40 cpv c.p. e la sua compatibilità con alcune figure criminose*, in *iusinitinere.it*, 2019).

## CAPITOLO IV

## PUNTI DI CONTATTO E DIVERGENZE TRA GDPR E D. LGS. 231/2001

SOMMARIO: 4.1. Confronto tra Modelli Organizzativi *Privacy* (MOP) e Modelli di Organizzazione, Gestione e Controllo (MOGC). – 4.2. L'approccio basato sulla valutazione dei rischi. – 4.3. *Accountability* e privilegio contro l'autoincriminazione. – 4.4. La colpa organizzativa e il principio dell'*accountability.* – 4.5. Prospettiva *de iure condendo*: il problema del *ne bis in idem*. – 4.6. Il *whistleblowing* tra GDPR e D. Lgs. 231/2001. – 4.7. Organi di sorveglianza a confronto: DPO (*Data Protection Officer*) e OdV (Organismo di Vigilanza). – 4.7.1. La qualificazione soggettiva dell'Organismo di Vigilanza ai fini della *privacy*. – 4.7.1.1. Il *Position Paper* dell'Associazione dei Componenti degli Organismi di Vigilanza *ex* D. Lgs. 231/2001. – 4.7.1.2. Il Parere del Garante per la protezione dei dati personali. – 4.7.2. DPO come membro dell'OdV, è ammissibile? – 4.7.3. Flussi informativi tra DPO e OdV. – 4.8. Le divergenze tra i Modelli.

Le realtà aziendali risultano essere destinatarie di due normative, il Regolamento (UE) 2016/679 e il D. Lgs. 231/2001, in forza delle quali adottano e attuano Modelli organizzativi[270], al fine di prevenire la commissione di reati presupposto ovvero le violazioni di diritti e libertà dei soggetti i cui dati vengono trattati.

Insieme a suddette normative merita di essere ricordata anche la disciplina in materia di sicurezza e salute del lavoratore, contenuta nel D. Lgs. 81/2008, la quale impone una serie di contenuti specifici che il Modello organizzativo *ex* D. Lgs. 231/2001

[270] Si precisa che l'adempimento del Regolamento (UE) 2016/679 è obbligatorio, di conseguenza anche l'adozione del Modello di organizzazione; viceversa, l'adempimento del D. Lgs. 231/2001 non è obbligatorio, sarà a discrezione dell'azienda adottare un Modello organizzativo, ricordando che l'attuazione e l'adozione efficace di quest'ultimo funge da esimente qualora emerga una responsabilità amministrativa da reato.

dovrà contenere a garanzia della sicurezza sul luogo di lavoro e che si interseca ed innesca assieme al GDPR e al Decreto 231, con simmetrici riverberi penali[271].

Dalla pratica tradizionale, nelle aziende si creano Modelli di organizzazione e gestione separati, indotti dalle differenti normative.

Secondo l'approccio tradizionale un'azienda si caratterizza per due *compliance* separate[272]. Per quanto attiene alla *compliance privacy*, con essa le imprese puntano ad adattarsi al GDPR, attraverso la definizione di una c.d. *roadmap*, ovverosia un documento che delinea le operazioni di adattamento da concludersi entro un termine prestabilito e che schematizza almeno i seguenti elementi inerenti all'azienda: strutture e uffici; soggetti coinvolti nel trattamento; cultura e competenze; processi e regole anche in riferimento alla gestione dei sistemi informativi; tecnologie e strumenti per la gestione della sicurezza informatica; sistemi di controllo; sistemi di *internal audit*[273]; documentazione sul trattamento dei dati. Nella strutturazione di un programma di *compliance*, prima di tutto, è necessario uno studio della situazione attuale, al fine di adeguare il sistema al GDPR; in questa prima fase ci si concentra sullo studio dei dati in relazione al capo di operatività dell'impresa, poiché ogni settore merceologico ha propri rischi tipici ed ogni azienda ivi operante ne ha, a sua volta, di peculiari. Questa fase ha un carattere continuativo, per cui le misure adottate per il trattamento dei dati personali sono riesaminate ed aggiornate, qualora ciò risulti necessario. L'impresa dovrà individuare una serie di informazioni

[271] I punti di contatto con il D. Lgs. 231/2001 si possono ravvisare nell'art. 30 del D. Lgs. 81/2008, secondo il quale se l'azienda dimostra di aver adottato ed applicato efficacemente un Modello di organizzazione e di gestione, questa viene sollevata dalla responsabilità amministrativa in caso di reato presupposto (omicidio colposo e lesioni personali colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro secondo il Decreto 231). Mentre, il contatto con il GDPR si può ravvisare in quanto nella gestione quotidiana della sicurezza sul luogo di lavoro, vi è, all'ordine del giorno, un trattamento di dati che rientra nell'ambito di applicazione del GDPR. Anzi, ci si potrebbe spingere ad affermare come spesso e volentieri sia proprio l'adempimento degli obblighi derivanti dal Decreto 81/2008 a determinare il sorgere di dati personali afferenti al dipendente, che impongono al datore di lavoro un corrispondente obbligo di trattamento sottoposto alla disciplina del GDPR. Si pensi, ad esempio, ai dati relativi allo stato di salute del dipendente, che normalmente derivano dallo svolgimento della sorveglianza sanitaria del medico competente e che danno luogo, oltre ad una cartella sanitaria e di rischio, anche ad un certificato di idoneità alla mansione. Documenti che, al loro interno, contengono dati concernenti lo stato di salute del dipendente e che, ricadendo pienamente nel perimetro di applicazione del GDPR, determinano in capo al datore di lavoro l'adozione degli adempimenti specifici prescritti dalla natura particolare del dato sanitario.

[272] Ci si riferisce alle *compliance* derivanti dal D. Lgs. 231/2001 e dal GDPR.

[273] vd. nota n. 263.

preliminari riguardanti il trattamento dei dati; in generale, sono comuni le seguenti informazioni: dati personali di consumatori e/o personale; come vengono raccolti i dati personali; perché vengono raccolti questi dati; come sono resi accessibili i dati; come sono conservati i dati; quali sono i rischi derivanti dal trattamento; quali sono i rischi derivanti dal mercato geografico in cui opera l'impresa; quali sono le problematiche dipendenti dal mercato internazionale; quale uso verrà fatto dei dati[274].

Nel sistema di *compliance* 231, *in primis*, si evidenzia che, per quanto concerne l'individuazione di una responsabilità amministrativa relativa al compimento di un reato commesso a vantaggio o nell'interesse dell'ente, appare fondamentale che la funzione *compliance* vada ad aggiornare periodicamente il catalogo dei reati presupposto conformandolo a quello aggiornato dal legislatore. La funzione *compliance* viene nominata e revocata da parte del Consiglio di Amministrazione e tra le finalità previste, oltre a quella di controllo della mera conformità normativa, vi è anche quella di consulenza alle altre funzioni operative della società stessa. Tali elementi differiscono con quelli previsti per l'Organismo di Vigilanza del D. Lgs. 231/2001, quest'ultimo, in quanto tale, non effettua attività di consulenza ed ha come finalità il controllo dell'adeguatezza e del rispetto del Modello *ex* D. Lgs. 231/2001. Pertanto, la funzione *compliance*, con riferimento al Modello 231, ha tra i suoi compiti sia quello di valutare la corretta conformità normativa sia quello di salvaguardare la società dal rischio di non conformità con riferimento ai danni reputazionali[275]. Per il tramite del procedimento di *compliance*, non si realizzerà nient'altro che un percorso capace di rendere la realtà aziendale responsabile, assumendo in prima persona obblighi e doveri afferenti alle attività e agli obiettivi perseguiti, aumentandone la solidità reputazionale, finanziaria e produttiva.

La visione tradizionale di separazione dei Modelli ha il fine di evitare rischi e costi

---

[274] cit. E. BARRACO, A. SITZIA, *GDPR in 10 punti*, IPSOA, Milano, 2018, pp. 20 e 21.

[275] cit. F. BIANCHI, op. cit., abstract. L'autore nel citato contributo chiarisce che la funzione *compliance* effettua controlli sulla conformità alle disposizioni di legge, ai provvedimenti delle Autorità di vigilanza e alle norme di autoregolamentazione, nonché a qualsiasi norma applicabile. L'azienda dovrà valutare i rischi di non conformità alle norme, per evitare di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni reputazionali, in conseguenza di violazioni a norme imperative (leggi, regolamenti) ovvero di autoregolamentazioni (statuti, procedure interne, codice di autodisciplina).

da mancata conformità, permette di ragionare a compartimenti stagni, di procedere all'esecuzione separata delle leggi e di costruire Modelli organizzativi differenti e separati.

Ormai detta visione è datata e considerata sconveniente, perché può comportare duplicazioni, sovrastrutture e appesantire gli apparati organizzativi. Ad oggi, si auspica la realizzazione di una *compliance* integrata che permetta di coordinare i vari Modelli di organizzazione e gestione.

Le diverse normative si prestano a letture simmetriche essendo unica la *ratio legis*: garantire sicurezza e prevenzione. Anche la struttura e il funzionamento dei Modelli hanno tratti omogenei sotto diversi aspetti, di conseguenza appare plausibile creare un unico Modello in forma integrata, in grado di soddisfare in sincronia tutte le normative. Allo stesso modo, non può tuttavia ignorarsi la sussistenza di divergenze tra i due contesti, sia con riferimento alle peculiari finalità perseguite dalla normativa in materia di *privacy*, sia in relazione all'entità degli obblighi sussistenti in capo agli enti.

La trama integrata dei diversi modelli è tessuta con mappature dei rischi unificabili, procedure plurivalenti, organismi di vigilanza e controllo (DPO e OdV) in comunicazione osmotica e sincrona tra di loro, riuniti in comitati periodici per la valutazione e gestione dei rischi. Il MOGC integrato è un'opportunità di sintesi innovativa per attuare la legalità d'impresa, che va solo intuita e colta[276].

Sperimentare questo nuovo approccio può arrecare differenti vantaggi: risparmiare; evitare duplicazioni procedurali e di controllo; garantire omogeneità e congruenza documentale.

Sarà compito di ogni realtà aziendale, tenendo conto delle attività svolte e dei rischi annessi, valutare se la struttura di fondo del Modello 231 adottato sia eventualmente compatibile anche per l'adempimento delle prescrizioni previste dal GDPR.

A tal proposito, questo capitolo, mettendo a confronto il GDPR e il D. Lgs.

---

[276] cit. M. CIRIGLIANO, *Dal D. Lgs. 231/2001 al GDPR (Regolamento UE 2016/679) attraverso il D. Lgs. 81/2008: il modello di organizzazione gestione e controllo integrato, avanguardia di un progetto di attuazione normativa combinata, un'opportunità per le aziende da intuire e cogliere*, in *Giurisprudenza penale web*, 1-*bis*, 2021, p. 2. Questo contributo si propone di capire se vi è la possibilità concreta di realizzare una *compliance* integrata per la *governance* aziendale, sostenendo che essa rappresenti il futuro.

231/2001, si pone l'obbiettivo di individuare e valorizzare eventuali punti di contatto tra le due discipline per sostenere un coordinamento reciproco, conveniente ed efficace, ma senza sorvolare ed evitare le divergenze quali ostacoli per l'integrazione. Analizzando i punti di contatto e le divergenze si potrà avere maggiore consapevolezza circa la possibilità di realizzare una *compliance* integrata e su come si potrà realizzare. Infine, si auspica un cambio di prospettive che sia tale da permettere una maggiore chiarezza, in aiuto delle realtà aziendali che si trovano di fronte a plurime normative da dover rispettare rigorosamente, pena l'applicazione di sanzioni di notevole entità, quando dette normative presentano punti di intersezione tali da permettere un loro coordinamento che eviterebbe diverse problematiche.

### 4.1. *Confronto tra Modello Organizzativo* Privacy *(MOP) e Modello di Organizzazione, Gestione e Controllo (MOGC)*

Il Modello Organizzativo *Privacy* (MOP) presenta diversi punti di contatto con le disposizioni dettate dal D. Lgs. 231/2001, quindi con il Modello di Organizzazione, Gestione e Controllo (MOGC). Tali denominatori comuni sono dati, essenzialmente, dalla presenza di alcuni fattori che si possono riassumere in: organigramma; approccio basato sull'analisi dei rischi; Codice etico; Organismi di controllo; piano di formazione; flussi informativi; procedura *data breach*; certificazioni; protocolli di formazione delle decisioni dell'organizzazione.

Come già analizzato, il MOP è un insieme di misure tecniche ed organizzative adeguate in grado di soddisfare il principio di *accountability*, per cui l'azienda dimostra di aver svolto azioni di responsabilizzazione per la prevenzione di trattamenti illeciti di dati e la conseguente violazione di diritti e libertà fondamentali. Il MOGC è un sistema che, se adottato ed attuato efficacemente, previene la realizzazione di illeciti all'interno dell'azienda e permette all'ente, nel caso detti illeciti siano commessi da soggetti che lo

compongono, di comprovare che la commissione del reato non è eziologicamente collegabile ad una sua "colpa organizzativa".

Analizzando nel dettaglio dette analogie si può ravvisare in entrambi i Modelli un organigramma, attraverso il quale si individuano e descrivono i ruoli assegnati, sulla base del criterio *Segregation of Duties* (SoD)[277]; quest'ultimo impone che un'organizzazione sia imperniata su di una segmentazione di ruoli e su di una responsabilità strutturata ed organica, tipizzando la separazione dei compiti, affinché nessuno possa gestire autonomamente un intero processo[278]. Perciò, occorre individuare distinte responsabilità in capo a ciascuna funzione, descrivendone nel dettaglio i compiti affidati.

Entrambi i Modelli organizzativi utilizzano un approccio basato sull'analisi dei rischi[279], in tal caso si possono ravvisare sia delle analogie che delle divergenze. I Modelli puntano a prevenire la realizzazione di reati informatici, attraverso l'analisi dei rischi, per cui vi è l'obbligo di provvedere all'individuazione e valutazione dei rischi associati alle varie attività svolte in ragione dei processi aziendali nell'ambito dei quali sono trattati i dati. Da ricordare, come già visto, nonostante il D. Lgs. 231/2001 non preveda all'interno del catalogo dei reati presupposti i reati di cui agli artt. 167 e ss. del Codice della *privacy* inerenti al trattamento illecito di dati, non esclude che i reati informatici, facenti parte del catalogo, abbiano delle ripercussioni lesive della riservatezza e dell'integrità dei dati personali. Le previsioni del Decreto 231, benché funzionali ad esonerare l'ente da responsabilità per reati commessi nel suo interesse o a suo vantaggio, erigono un sistema di tutela "indiretta" anche per i diritti e le libertà dei titolari dei dati personali soggetti a trattamento, andando così ad integrare gli adempimenti previsti dal GDPR[280].

---

[277] Il criterio *Segregation of Duties* trae essenzialmente origine dal pensiero del filosofo francese Montesquieu, secondo il quale: «*Chiunque abbia potere è portato ad abusarne: egli arriva sin dove non trova limiti. Perché non si possa abusare del potere occorre che il potere arresti il potere*».

[278] cit. C. E. PONTI, S. PERSI e M. A. PEREGO, *Il modello organizzativo privacy – MOP*, Giuffrè, 2020, pp. 57 ss.

[279] Detto anche, in inglese "*risk based approach*".

[280] cit. D. COSTA, *I modelli 231 e la compliance aziendale sulla tutela dei dati personali. Aspetti comuni e divergenze a quattro anni di distanza dall'entrata in vigore del GDPR*, in *Giurisprudenza penale web*, 2020, p. 2. L'autore fa notare che, per esempio, nei reati informatici di cui agli art. 615-*ter*, 617-*quinquies* e 635-*ter* c.p., considerati delitti presupposto *ex* art. 24-*bis*, non si può negare l'elevato tasso di rischio per la riservatezza e l'integrità dei dati personali, determinato dall'accesso abusivo ad un sistema

La mappatura dei rischi, vista la sua estrema importanza, verrà analizzata nel dettaglio al paragrafo successivo. Anticipando brevemente ciò che verrà in seguito affrontato, vi è chi ravvede plurime analogie a tal proposito tra i due Modelli tali da permettere di procedere ad una mappatura unificata che abbracci tutti i rischi aziendali, dal rischio di *data breach* al rischio di commissione di reati presupposto, evitando duplicazioni, sovrapposizioni e stratificazioni che altrimenti si realizzerebbero utilizzando due mappature separate. Di converso, vi è chi sottolinea le differenze tra i due approcci gestionali, le quali sembrerebbero di ostacolo ad una mappatura dei rischi integrata.

Il Codice etico è uno dei punti di partenza della corretta applicazione del D. Lgs. 231/2001, è un elemento essenziale in un MOGC efficace. Il documento contiene l'insieme dei principi cardine della politica aziendale che vengono poi calati nel concreto con protocolli di prevenzione.

Anche il GDPR prevede che l'adeguatezza dei Modelli ed il rispetto degli obblighi in capo all'ente ed al titolare del trattamento possano essere dimostrati mediante l'adesione a determinati codici di condotta, anche detti codici etici, elaborati dagli organi rappresentativi degli enti o dei titolari del trattamento ai sensi dell'art. 40 del GDPR[281]; viene considerato quale misura di *accountability*, supportato da adeguata formazione ed eventualmente dei test per valutare la consapevolezza dei destinatari.

Si delineano una serie di regole contenenti i comportamenti richiesti e quelli vietati a tutti i soggetti coinvolti, tramite soluzioni descrittive ovvero attraverso un supporto di esempi che illustrano le norme di comportamento e gli esempi di non conformità al Codice, ciò permette di ridurre i rischi aziendali attraverso la forza del monito etico.

Il Codice etico introduce i valori sui cui si basa l'etica dell'organizzazione completandosi con un sistema sanzionatorio commisurato sulla base della gravità delle eventuali infrazioni commesse.

---

informatico, così come l'istallazione di un *software* (per esempio, un c.d. *trojan*) e altri programmi che acquisiscono fraudolentemente comunicazioni informatiche o danneggiano sistemi operativi.

[281] cit. *Ibidem*, p. 4.

La duttilità di detto strumento lo rende per definizione materia ideale da plasmare in un'ottica multidisciplinare, si presta ad essere progettato con una visione integrata per evitare smarrimenti dovuti dalle differenti normative.

Un'ulteriore analogia è caratterizzata dagli Organismi di controllo previsti dal Decreto 231 e dal GDPR. I Modelli di prevenzione dei reati e le misure organizzative a tutela della liceità dei trattamenti dati non possono considerarsi adeguati senza idonei centri di imputazione di compiti di sorveglianza, affinché gli strumenti di *compliance* siano adottati ed efficacemente implementati. Detti centri di imputazione vengono identificati nell'Organismo di vigilanza (OdV) e nel *Data Protection Officer* (DPO)[282]. Ad entrambi dev'essere garantita una piena autonomia, devono caratterizzarsi per una condizione di terzietà ed indipendenza, si affidano poteri di controllo circa la legalità sul funzionamento dell'ente e si assicurano dei flussi informativi che l'ente o i protagonisti del trattamento dati devono assicurare con oggetto le eventuali violazioni[283]; in tal modo, queste figure vengono responsabilizzate dato che le loro attività prevedono necessariamente un trattamento di dati.

Verrebbe naturale, viste le analogie, pensare di poter cumulare questi ruoli in un unico soggetto monocratico o collegiale, ma anche in tal caso vi è chi ravvede delle differenze che dipendono dai diversi obbiettivi perseguiti. Inoltre, si è sviluppato un annoso dibattito circa la qualificazione di detti soggetti, in particolare, sulla qualificazione soggettiva dell'Organismo di vigilanza ai fini *privacy*.

A tal proposito, il confronto tra DPO e OdV merita un approfondimento che verrà affrontato nei paragrafi successivi, con l'obbiettivo di comprendere se detti organi possano coincidere oppure si caratterizzino da elementi tali da renderli incompatibili.

Il piano di formazione rappresenta una misura atta a consentire di applicare in maniera efficace i Modelli. Il GDPR, agli artt. 29 e 32, stabilisce che il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai dati personali, debba essere istruito in tal senso dal

[282] cit. *Ibidem*, p. 7.
[283] *Ex* art. 6, comma 2, lett. b) del D. Lgs. 231/2001 e artt. 37 e 38 del GDPR.

titolare del trattamento. Il Decreto 231 all'art. 6 prevede come condizione necessaria, affinché il Modello sprigioni l'efficacia esimente è la sua efficace attuazione che si realizza attraverso un'adeguata formazione del personale aziendale in merito alla disciplina di legge e ai contenuti del MOGC adottato dalla società.

Seguendo l'approccio tradizionale si creano moduli di formazione separati per pacchetto normativo, i quali vengono solitamente vissuti con fastidio dall'organico aziendale, che si sente distolto dall'operatività quotidiana ed obbligato a subire, spesso in sequenza, la somministrazione di formazione a tema. La formazione viene concepita ed accettata come una terapia dolorosa ma necessaria a cui non ci si può sottrarre[284].

A tale riguardo, si prospetta la possibilità di attuare una formazione plurivalente e multidisciplinare che riguarda entrambi i Modelli, conveniente a livello di costi e sicuramente più tollerata ed accettata dalla popolazione aziendale che riuscirebbe così ad acquisire una visione di insieme.

I flussi informativi costituiscono un punto di contatto tra il MOP e il MOGC. Il D. Lgs. 231/2001 esige un'organizzazione che preveda flussi informativi verso l'Organismo di Vigilanza[285]; simmetricamente, il GDPR prevede che il *Data Protection Officer*, soprattutto se esterno, subito dopo la presa in carico dei compiti di sorveglianza in un'organizzazione, dovrà attivare meccanismi per essere costantemente informato su cosa accade in azienda e per evitare di tralasciare nuove attività rilevanti che possono richiedere un aggiornamento dell'impianto *privacy*, come, per esempio, un aggiornamento dell'analisi dei rischi o dello svolgimento della valutazione di impatto della protezione di dati[286].

I flussi informativi rivolti all'OdV si compongono di informazioni necessarie

---

[284] cit. M. CIRIGLIANO, op. cit., p. 12. Rispetto a detto argomento, il contributo sottolinea come le aziende vadano a somministrare a dosi inesorabili, obbligatori moduli formativi in materia di salute e sicurezza sul lavoro, in materia di *privacy* e sul D. Lgs. 231/2001, almeno annuali e con un test di fine corso per comprovare il passaggio dei contenuti del docente (spesso virtuale) al succube discente.

[285] *Ex* art. 6, comma 2, lett. d) del D. Lgs. 231/2001: «*In relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, i modelli di cui alla lettera a), del comma 1, devono rispondere alle seguenti esigenze: […] d) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli […]*».

[286] Anche detta, in inglese: *Data Protection Impact Assessment* (DPIA).

affinché possa svolgere i suoi compiti. Fermo restando l'obbligo di riservatezza relativamente alle informazioni acquisite, l'OdV deve avere libero accesso a tutte le informazioni della società, senza necessità di alcun consenso preventivo. Inoltre, l'OdV, grazie a flussi informativi opportunamente strutturati, viene a conoscenza delle vicende dell'ente rilevanti in termini di *compliance*; infatti, il novero delle informazioni non comprende soltanto quelle di natura economico-finanziaria, ma anche, ad esempio, informazioni relative all'attività produttiva e commerciale, sviluppi nella tecnologia, emanazione di norme e regolamenti che potrebbero avere impatto sull'attività aziendale.

Mentre, per quanto riguarda i flussi informativi rivolti al DPO, quest'ultimo dovrà essere informato delle nuove iniziative o progetti che potrebbero impattare sulle modalità o finalità di trattamento dei dati personali, come ad esempio nel caso in cui sia adottato un nuovo sistema IT o vengano esternalizzati dei servizi. Non è compito di chi comunica le innovazioni preoccuparsi del trattamento dei dati o se l'attività è significativa per la *privacy*, sarà compito del DPO valutarlo. Attivare i flussi informativi è la fase conclusiva della presa in carico; da questo punto il DPO è pronto a esercitare il suo ruolo di consulenza e controllo[287].

Per concludere, un Modello integrato si baserebbe su flussi informativi sincroni attraverso un dialogo strutturato e periodico fra i *controller* che le diverse leggi designano, creando, eventualmente, efficaci comitati di controllo.

Punti di collegamento tra i due modelli emergono anche in relazione alle procedure da adottare per rilevare e segnalare eventuali infrazioni. La procedura di *data breach* prevista dal GDPR[288] risponde alle stesse esigenze che il Modello 231 impone allorché sussista l'obbligo di fornire informazioni o segnalare anomalie. La procedura relativa al *data breach* potrebbe considerare anche la segnalazione dell'evento all'Organismo di Vigilanza che ha lo scopo di istituire chiari e identificati canali informativi idonei a garantire la ricezione, l'analisi e il trattamento di segnalazioni, anche

[287] cit. P. CALVI, *DPO la presa in carico di un'azienda: le fasi di assessment*, in *cybersecurity360.it*, 2021.

[288] *Ex* art. 33 del GDPR.

in forma anonima, relative alle violazioni del Modello e/o del Codice etico e di definire le attività necessarie alla loro corretta gestione.

Da differenziare rispetto ai codici di condotta vi sono le certificazioni, rilasciate da appositi organismi a comprova della determinazione di sistemi organizzativi idonei a prevenire illeciti penali o danni di dati personali. Si vede come la funzione di dette certificazioni si esplica in entrambi i Modelli, anche se si ravvisa un diverso grado di efficacia. Gli artt. 24 e 32 del GDPR stabiliscono che il titolare del trattamento può dimostrare l'osservanza degli obblighi e la predisposizione di garanzie appropriate per la tutela dei dati personali mediante il ricorso ai meccanismi di certificazione disciplinati all'art. 42 del Regolamento. Si pensi, alla certificazione ISO 27001 che rappresenta lo standard internazionale di sicurezza delle informazioni più rilevante e definisce le *best practices*, i requisiti logici, fisici e organizzativi necessari per impostare e gestire un sistema di gestione della sicurezza delle informazioni[289]. Secondo la giurisprudenza, le certificazioni rilasciate da istituti quali la *International Standard Organization*, non possono ritenersi equivalenti ai Modelli 231, al fine di esonerare l'ente dalla responsabilità amministrativa da reato[290]. Mentre, dette certificazioni nel Modello *privacy*, sono strumenti particolarmente efficaci per la prevenzione di reati informatici, si definiscono come misure di *accountability* e mitigano i rischi di perdita di riservatezza, disponibilità ed integrità dei dati, garantendo una tutela e protezione dei dati personali e delle informazioni trattate dall'ente.

Il Decreto 231 non prevede le certificazioni come obbligatorie, dunque, non hanno un'automatica efficacia esimente. Il GDPR da la possibilità al titolare di dotarsi di una certificazione di processo da utilizzare a dimostrazione di aver rispettato delle prescrizioni normative ma che, pur se espressamente prevista, non ha, da sola, efficacia esimente. La certificazione agevola l'applicazione concreta delle prescrizioni normative,

---

[289] cit. D. COSTA, op. cit., p. 5.

[290] vd. Cass. pen, sez. VI, 13 settembre 2017, n. 41768, sent., in materia di infortuni sul lavoro e reati ambientali, secondo cui «*non possono essere ritenuti equivalenti ai modelli richiesti dal D. Lgs. n. 231 del 2001, perché non contenevano l'individuazione degli illeciti da prevenire unitamente alla specificazione del sistema sanzionatorio delle violazioni del modello e si riferivano eminentemente al controllo della qualità del lavoro nell'ottica del rispetto delle normative sulla prevenzione degli infortuni sul lavoro o degli interessi tutelati dai reati in materia ambientale*».

ma il suo ruolo è anche quello di costituire una lista di controllo per il verificatore o l'inquirente che si troverà già di fronte un percorso di indagine quasi cristallizzato e che potrebbe, a seconda dei casi, determinare l'applicazione di una sanzione ovvero la constatazione che non vi sia "nulla da rilevare"[291].

Entrambe le legislazioni si preoccupano di indicare ai propri destinatari di adottare dei protocolli standardizzati per la formazione e l'esecuzione delle decisioni dell'organizzazione e/o del trattamento dati che garantiscono una conformità alla normativa, sia essa quella penale piuttosto che quella in materia di *data protection*, che sussista già a monte dell'intero procedimento decisionale[292].

L'art. 6, comma 2, lett. b) del D. Lgs. 231/2001 suggerisce all'ente: «*prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire*», lasciando agli organi sociali la determinazione del contenuto di detti protocolli. Ugualmente, il legislatore europeo ha individuato le misure tecniche ed organizzative che assicurano un'adeguata tutela ai dati degli interessati, in particolare, l'art. 25 del GDPR nel definire la *privacy by design* al comma 1 e la *privacy by default* al comma 2 , fa riferimento all'adozione, da parte del titolare del trattamento, di «*misure tecniche e organizzative adeguate, in modo da attuare efficacemente i principi di protezione dei dati e da garantire nel trattamento i requisiti del Regolamento e la tutela dei diritti degli interessati*». Si ravvisa un'armonia tra le due disposizioni che, pur normando aspetti differenti di *compliance,* convergono sulla necessità di adottare delle prassi per garantire la conformità delle attività aziendali alle normative vigenti e vagliare i rischi sottesi a tali attività, c.d. *risk-based approach* prerequisito per individuare misure tecniche e organizzative adeguate.

[291] cfr. L. LUPARIA [et. al.], A. MONTI (a cura di), op. cit., pp. 237 e 238.
[292] cit. D. COSTA, op. cit., p. 5.

### 4.2. *L'approccio basato sulla valutazione dei rischi*

Come già detto, la gestione della *compliance* aziendale presuppone in tutti i settori un approccio basato sulla responsabilizzazione dei soggetti e un metodo di analisi basato sul rischio, coerente con i presidi aziendali predisposti. Il medesimo approccio al rischio si ha anche nell'ambito della tutela dei dati personali; secondo quanto previsto dal GDPR, si applica una tutela preventiva, basata sulla responsabilizzazione del titolare e del responsabile del trattamento, con un'analisi dei rischi su tutti i trattamenti effettuati e con il ricorso, se necessario, alla valutazione di impatto sulla protezione dei dati personali in un'ottica di *privacy by design* e *by default*.

Da un lato si procede alla valutazione e mappatura dei rischi collegati alla commissione di reati presupposto, dall'altro lato dei rischi collegati alle violazioni nel trattamento dei dati. In tal modo si individua una soglia di rischio accettato, sulla base della quale compiere scelte organizzative idonee a scongiurare eventi avversi. A tal proposito, si sviluppano due opinioni, vi è chi ravvede plurime analogie tali da permettere di realizzare una mappatura unica in grado di coinvolgere tutti i rischi aziendali, evitando sovrapposizioni e stratificazioni, ed essendo meglio monitorabile ed implementabile; viceversa, vi è chi evidenzia le differenze tra i due approcci, le quali sembrerebbero impedire la realizzazione di una mappatura integrata.

Attraverso la mappatura del rischio di perfezionamento dei reati informatici, con una metodologia integrata c'è la possibilità di individuare e pesare sia i profili di rischio rilevanti al fine di prevenire ipotesi di responsabilità amministrativa dell'ente alla luce del D. Lgs. 231/2001, sia i profili di rischio inerenti alla *privacy* (GDPR) ma anche i riverberi collaterali sul *business* e quelli reputazionali[293]. Altresì, tale approccio consente di riportare sotto un comune denominatore i profili connessi alla responsabilità dell'ente che, colposamente, abbia omesso di predisporre una struttura societaria funzionale ad evitare la commissione di *data breach* o di reati *ex* D. Lgs. 231/2001 e che, in entrambi i casi, comporta l'irrogazione di pesanti sanzioni pecuniarie nei confronti dell'impresa e

[293] cit. M. CIRIGLIANO, op. cit., p. 6.

viene invece esclusa, o attenuata, qualora l'ente o il titolare del trattamento abbia predisposto adeguate misure di prevenzione[294].

In capo al titolare e al responsabile del trattamento gravano una serie di obblighi previsti agli artt. 24 e 32 del GDPR[295], secondo i quali detti soggetti devono porre in essere le misure tecniche ed organizzative adeguate e proporzionate ai rischi derivanti dalla distruzione, dalla modifica, dalla divulgazione non autorizzata, dalla perdita o dall'accesso non autorizzato ai dati personali, al fine di garantire un idoneo livello di sicurezza e per essere in grado di dimostrare che il trattamento viene effettuato conformemente al GDPR. In capo all'ente vi è l'onere, ai sensi dell'art. 6, comma 1, lett. a) del Decreto 231, di adottare ed attuare efficacemente, ad opera del proprio organo dirigente e prima della commissione del fatto di reato, modelli di organizzazione e gestione idonei a prevenire i reati della specie di quello verificatosi, la cui prova avrà efficacia esimente nei confronti dell'ente; in particolare, il medesimo articolo al comma

---

[294] cit. D. COSTA, op. cit., p. 3.

[295] *Ex* art. 24 del GDPR: «*1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario. 2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento. 3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento*». *Ex* art. 32 del GDPR: «*1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. 2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. 3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. 4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*».

2, lett. a) stabilisce: «*In relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, i modelli di cui alla lettera a), del comma 1, devono rispondere alle seguenti esigenze: a) individuare le attività nel cui ambito possono essere commessi reati […]*», per cui l'attività di mappatura dei rischi, attraverso l'individuazione delle aree d'attività più sensibili e dei reati che potrebbero essere commessi, rappresenta la *condicio sine qua non* dell'adeguatezza del Modello 231.

Secondo quanto disposto dal Regolamento (UE) 2016/679, vi sono tre livelli di valutazione del rischio: valutazione generica e non formalizzata *ex* art. 24 e 35 del GDPR, collegata all'esigenza di effettuare trattamenti che siano il minimo lesivi ed impattanti sui soggetti interessati; se il trattamento è suscettibile di provocare un rischio elevato per i diritti e le libertà delle persone fisiche, presuppone una valutazione di impatto sulla protezione dei dati; se il risultato della valutazione restituisce un rischio elevato che non può essere mitigato dall'adozione di ulteriori misure aggiuntive, necessita il riscorso ad una valutazione preventiva da parte dell'Autorità di controllo.

Nel Regolamento la centralità dell'analisi del rischio si può evincere anche nel contesto dell'art. 35, ossia nella *Data Protection Impact Assessment* (DPIA) che il titolare deve effettuare quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Inoltre, rientrano nel confronto anche gli obblighi di riesame e l'eventuale aggiornamento dei Modelli, attraverso procedure di revisione delle misure tecniche ed organizzative e delle garanzie necessarie *ex* art. 24 e 35 del GDPR, ovvero per assicurare l'efficace attuazione del Modello a seguito di violazioni o di mutamenti dell'organizzazione *ex* art. 7, comma 4 del Decreto 231.

La gamma dei rischi si apprende solitamente attraverso un sistema costituito da interviste ai principali attori dello scenario aziendale, spesso completato da un sistema informatico che ne elabora i risultati e produce una mappa e una pesatura di detti rischi. Si possono utilizzare tecniche *Risk Self Assessment* (RSA) per la valutazione del rischio potenziale collegato ad eventi di non conformità, il quale ben si adatta ad entrambi i contesti normativi sfruttando le sinergie al fine di rappresentare una valutazione più

completa che riguarda: andamento delle perdite operative dovute ad eventi di non conformità; impatto sulla componente reputazionale, valutando i suoi possibili effetti su deterioramento o perdita di relazione con il cliente; conseguenze sul fatturato, rilevanza mediatica dei fattori generatori di rischio. Quindi, si auspica l'utilizzo di un sistema di mappatura integrato, omogeneo e sinergico, chiamato dagli esperti *Enterprise Risk Management*[296].

Per concludere, sulle considerazioni appena esaminate si basano i sostenitori dell'applicazione di una valutazione dei rischi integrata, in grado di contenere sia i rischi connessi alla commissione di un reato presupposto sia i rischi connessi alle violazioni nel trattamento dei dati personali, la quale realizzerebbe un *saving* di costi e di tempo per l'azienda permettendo un monitoraggio più agevole e una conseguente implementazione nel caso di mutamenti esogeni (derivanti dagli scenari normativi) ovvero endogeni (mutamenti organizzativi e di *business*).

Come più volte ripetuto, vi è anche chi sostiene che l'analisi del rischio sia uno degli esempi più evidenti delle differenze fra i due approcci gestionali. L'approccio previsto dal GDPR è "di *default*" i dati personali devono poter circolare, salvo adottare il minimo indispensabile di restrizioni che raggiunge un compromesso accettabile fra i diritti dell'interessato e quelli del titolare del trattamento. L'attività di prevenzione richiesta da D. Lgs. 231/2001 è, invece, diretta a prevenire fatti umani, della natura più disparata, e non l'incremento della probabilità del loro verificarsi il che limita fortemente la rilevanza di un'analisi del rischio in ambito 231[297].

Nella valutazione dei rischi si deve considerare, oltre la probabilità che accadano eventi avversi, anche la probabilità che determinate scelte aziendali possano violare prescrizioni normative. Dunque, bisogna considerare un'importante variabile: l'entità

---

[296] Il modello ERM (*Enterprise Risk Management*) proposto dal *Committee of Sponsoring Organization of the Treadway Commission* (CoSO) si scompone di cinque elementi fortemente interconnessi fra loro: *Governance and Culture*; *Strategy and Objective Setting*; *Performance*; *Review and Revision*; *Information and Communication Reporting*.

[297] cit. L. LUPARIA [et. al.], A. MONTI (a cura di), op. cit., p. 230. Nella medesima pagina viene riportato un detto paradossale, ma indicativo, che circola nella comunità degli esperti di sicurezza informatica, del Professor Eugen Spafford: «*the only system which is truly secure is one which is switched off and unplugged locked in a titanium lined safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then, I wouldn't stake my life on it*».

delle sanzioni derivanti da determinate scelte. Questo perché, se i costi di sicurezza necessari per ridurre la pericolosità dei trattamenti fossero superiori alla sanzione attesa, il titolare del trattamento potrebbe decidere di assumersi l'alea di una conformità normativa meno rigorosa che, però, permetterebbe di realizzare un risparmio di costi immediato a fronte di una sanzione la cui configurabilità e irrogazione sarebbe incerta *an et quando*.

Quindi, non è detto che la riduzione del rischio di violazioni nel trattamento dei dati personali conforme al Regolamento produca automaticamente l'effetto esimente, qualora dette violazioni rilevassero anche ai sensi del Decreto 231. Viceversa, nel caso di prevenzione dei reati presupposto le scelte organizzative sono finalizzate ad ottenere in concreto l'efficacia esimente e dunque sono intrinsecamente idonee a raggiungere il massimo risultato, comportando anche una riduzione di possibili violazioni nel trattamento.

Il Decreto 231 stabilisce che l'esimente possa operare solo qualora l'ente prevenga effettivamente la commissione dei reati presupposto, non se ne riduca la probabilità di accadimento, come invece si richiede quando opera come titolare del trattamento; l'obbiettivo è di far in modo che se dovessero accadere illeciti, accadano al di fuori del perimetro di controllo dell'ente stesso.

Un'ulteriore differenza attiene alla natura della minaccia. Per quanto riguarda il GDPR le minacce dovranno essere ricercate negli errori di progettazione e gestione dei sistemi informativi e, in misura minore, nei soggetti potenzialmente interessati a conoscere le informazioni, ovvero a renderle indisponibili al titolare; mentre, nel Modello 231 le minacce di cui si deve tener conto sono interne perché derivanti dai soggetti interni, apicali o sottoposti, potenziali autori delle condotte illecite rilevanti. Nel primo caso ci si concentrerà nei processi aziendali, nel secondo caso ci si concentrerà oltre che nella disamina dei processi anche nei comportamenti tenuti dalle persone.

Per concludere, sulla base delle osservazioni appena sollevate risulta complicato creare un modello unitario che integri GDPR e Decreto 231 stante i differenti presupposti ed obbiettivi delle analisi del rischio condotte in entrambi gli ambiti, sottolineando il concetto secondo cui la riduzione del rischio ai sensi del Regolamento non implica

necessariamente che le misure adottate per tale fine siano in grado di costituire esimente ai sensi del Decreto. Bisogna verificare attentamente che l'analisi del rischio attuata dall'azienda riesca a scongiurare le violazioni nel trattamento dei dati personali e, allo stesso tempo, fungere da esimente per la responsabilità amministrativa da reato.

### 4.3. Accountability *e privilegio contro l'autoincriminazione*

L'esercizio del diritto di difesa nei procedimenti amministrativi azionati dal Garante per la protezione dei dati personali e nei procedimenti penali promossi dal Pubblico Ministero è condizionato dalla struttura dei rispettivi Modelli di organizzazione, gestione e controllo.

Il Modello 231 ha una precisa *ratio*: evitare il coinvolgimento dell'ente, titolare del trattamento, in azioni illecite commesse dai soggetti che lo compongono. Inoltre, nel caso di indagine penale, non è tenuto a cooperare con gli inquirenti, fatti salvi i doveri di dissuadere i soggetti apicali o sottoposti dal commettere i reati di ostruzione della giustizia.

Il Modello *privacy* si propone di documentare le scelte effettuate in materia di trattamento dei dati per scongiurare l'applicazione delle sanzioni irrogate dall'autorità nazionale di protezione dei dati e, addirittura il potenziale avvio di un procedimento penale. Le sanzioni amministrative rivestono un ruolo preminente che riduce sensibilmente la possibilità di esercitare il diritto di difesa, essendo quest'ultimo una prerogativa riconosciuta in sede penale.

Nel Modello *privacy* vige il dovere di *accountability*[298] che può entrare in conflitto con diversi diritti fondamentali in materia penale, ed in particolare con il privilegio contro l'autoincriminazione[299]. Il dover dar conto delle proprie carenze organizzative,

[298] Per un approfondimento sul principio di *accountability* vd. paragrafo 2.2.7.

[299] Mutuando le categorie proprie dell'ordinamento di *common law*, la dottrina italiana riconosce all'accusato il c.d. *privilege against the self-incrimination* per cui si garantisce alla persona che si trovi priva di una formale accusa (testimone, persona informata sui fatti, persona sottoposta ad ispezione o ad una inchiesta amministrativa) possa essere costretta a fornire un contributo conoscitivo che porti alla propria

nell'ipotesi di condotte che possono dar luogo ad una responsabilità penale, può esporre colui al quale è attribuito questo dovere ad un obbligo di "auto-denuncia", oppure all'obbligo di presentare prove contro di sé, in conflitto con il più basilare diritto di difesa e a sovversione dell'onere della prova[300]. Quindi, il Modello previsto dal GDPR si può definire come autoincriminatorio, per via del ruolo primario che riveste il principio dell'*accountability*.

Il principio di *accountability* dovrebbe essere applicato fino al punto in cui non superi la soglia del *nemo tenetur se detegere*[301].

Nell'affrontare questa problematica si cercano delle soluzioni, a titolo esemplificativo, si può analizzare il *Data Protection Act* del 2018 del Regno Unito, che prevede all'art. 20, rubricato "*self incrimination"*, un'esenzione specifica dall'obbligo di fornire informazioni, nel caso in cui queste possano portare all'incriminazione del titolare del trattamento.

L'art. 24 del Regolamento (UE) 2016/679 pone a carico del titolare del trattamento un notevole fardello, poiché esso ha l'onere di verificare se al suo interno si verificano degli "incidenti" organizzativi che possono esporre i diritti, garantiti dalla normativa in tema di trattamento dei dati personali, ad una violazione. Tra questi doveri stabiliti in via generale, ve ne è anche uno esplicito e direttamente sanzionato, ossia il dovere di notificare al Garante per la protezione dei dati personali, ed in alcuni casi anche agli stessi interessati, entro un termine perentorio la (anche solo potenziale) violazione della riservatezza dei dati in conseguenza del c.d. *data breach*[302].

La delicatezza del problema è ancora più evidente se si considera che le verifiche

---

incriminazione. Principio che trova indiretto fondamento negli articoli 24, 27, 111 Cost. e nell'art. 6 CEDU, nell'art. 47 CDFUE (cfr. A. FABERI, op. cit., p. 10).

[300] cit. A. FABERI, op. cit., p. 4.

[301] L'espressione *nemo tenetur se detegere* descrive un contegno che l'accusato di un reato può assumere rispetto ad un'accusa penale formulata nei suoi confronti. Essa ricomprende il diritto di astenersi dal rendere informazioni nel caso in cui queste possano, anche solo astrattamente, esporre il medesimo ad una incriminazione e il correlato dovere della pubblica autorità di astenersi dall'ottenere una dichiarazione auto-incriminante con metodi coercitivi o con l'inganno, ovvero senza il previo avvertimento delle conseguenze cui il cittadino si espone con il rendere le informazioni dinnanzi all'autorità stessa (cit. *Ibidem*, p. 9).

[302] cit. *Ibidem*, pp. 18 e 19.

di conformità al GDPR sono, di regola, compiute da soggetti appartenenti al Corpo della Guardia di finanza, i quali possiedono la qualifica di agenti e ufficiali di polizia giudiziaria che potrebbe implicare, senza soluzione di continuità, il passaggio dalla verifica amministrativa ad attività di iniziativa, come il sequestro probatorio a seguito della constatazione della possibile commissione di reati non necessariamente connessi al trattamento dei dati personali[303]. A tal proposito, la giurisprudenza, formatasi essenzialmente nella materia fiscale e tributaria, nel passaggio da attività amministrativa ad attività di iniziativa penale, ha legittimato la trasmigrazione degli atti di accertamento nel fascicolo del Pubblico Ministero, anche se non compiuti nel rispetto delle garanzie difensive, essendosi svolti in seno ad un procedimento amministrativo[304].

Da considerare vi è anche l'art. 220 disp. att. c.p.p. secondo il quale si riconosce che anche nella fase dei controlli meramente amministrativi, purché siano emersi gli indizi di una responsabilità penale, siano anticipate le garanzie fondamentali previste dal codice per la raccolta delle prove. L'interpretazione letterale di detta norma, denota un difetto di tutela rispetto al *nemo tenetur*, poiché nel caso concreto è proprio l'obbligo di cooperazione che farebbe emergere nuovi indizi di reato. Se emerge una responsabilità penale, l'obbligatorietà della collaborazione è contraria al principio del privilegio di non autoincriminarsi, con la conseguenza che, qualora detta collaborazione manchi, il soggetto sarà sottoposto ad una sanzione, sia in sede penale che amministrativa, considerata illegittima.

Anche la Corte europea dei diritti dell'uomo si pronuncia nel senso che il principio *nemo tenetur se detegere* si debba applicare anche al di fuori del processo penale in senso stretto, estendendosi alla fase prodromica di accertamento della violazione di natura non solo penale, ma anche amministrativa, proprio nella fase dedicata alla collaborazione. Questa estensione delle garanzie difensive nei confronti di coloro che sono sottoposti a sanzioni amministrative, si giustifica sulla base che dette sanzioni si caratterizzano per una finalità punitiva e, dunque, per una natura sostanzialmente penale[305].

---

[303] cit. L. LUPARIA [et. al.], A. MONTI (a cura di), op. cit., p. 245.
[304] vd. Cass. civ., sez. VI, 9 luglio e 28 settembre 2020, 20358, ord.
[305] La statuizione secondo cui le sanzioni amministrative, gravi e aventi una finalità punitiva si

Quindi, rispetto alla reale natura delle sanzioni previste per la commissione di illeciti amministrativi, aspetto fondamentale nel discorso in esame, la Corte Costituzionale numero 84 del 30 aprile 2021 ha stabilito l'illegittimità dell'art. 187-*quinquiesdecies* del D. Lgs. 58/1998[306] «*nella parte in cui si applica anche alla persona fisica che si sia rifiutata di fornire alla CONSOB risposte che possano far emergere la sua responsabilità per un illecito passibile di sanzioni amministrative di carattere punitivo, ovvero per un reato*». Le sanzioni amministrative di carattere punitivo sono state definite dalla Corte europea dei diritti dell'uomo, nella sentenza *Engel e altri* contro *Paesi Bassi* dell'8 giugno 1976, come solo formalmente amministrative, ma che, per la loro natura afflittiva, sono a tutti gli effetti considerate penali[307], soprattutto per quanto attiene ai diritti da garantire alla persona soggetta al procedimento.

L'art. 33 del GDPR impone al titolare del trattamento di notificare al Garante della *privacy* la violazione della riservatezza dei dati in conseguenza di un *data breach*; la violazione di suddetto obbligo di notifica espone il titolare ad una responsabilità, tanto per i reati in materia *privacy* eventualmente commessi, quanto per le sanzioni stesse che possono essere irrogate nel caso di omessa segnalazione. Analizzando l'art. 83 del GDPR[308] le sanzioni previste a carico del trasgressore si possono qualificare come penali. Le sanzioni si applicano sulla base di una serie di criteri utilizzati per valutarne la gravità,

---

debbano considerare sostanzialmente penali e perciò vi si applicano le garanzie difensive si riconduce alla pronuncia della Corte di Strasburgo nel caso *Engel e altri c. Paesi Bassi* (vd. Corte eur. Dir. uomo, 8 giugno 1976, *Engel e altri c. Paesi Bassi*; Id., 21 febbraio 1984, *Öztürk c. Germania*; Id., 24 febbraio 1994, *Bendenoun c. Francia*, 23 novembre 2006, *Jussila c. Finlandia*; Id., 4 marzo 2013, *Grande Stevens c. Italia*; Id., 15 novembre 2016, *A. e B. c. Norvegia*). Con queste pronunce la Corte EDU abbandona i criteri di classificazione formali ed elabora dei criteri sostanziali per stabilire se una sanzione formalmente amministrativa sia in realtà espressione della potestà punitiva dello Stato. L'approccio sostanzialistico elaborato dalla Corte EDU si impone anche negli ordinamenti nazionali e ha determinato l'avvio di un processo di assimilazione fra pene in senso stretto e sanzioni amministrative punitive.

[306] Testo unico delle disposizioni in materia di intermediazione finanziaria, ai sensi degli articoli 8 e 21 della legge 6 febbraio 1996, n. 52.

[307] A tal proposito, merita di essere citata anche la Sentenza del 20 marzo 2018, nella causa C-537/16 della Corte di giustizia dell'Unione Europea: «[…] *il diritto al silenzio* […] *è destinato ad applicarsi nel contesto di procedure suscettibili di sfociare nell'inflizione di sanzioni amministrative presentanti carattere penale. Per valutare tale carattere penale rilevano tre criteri. Il primo è dato dalla qualificazione giuridica dell'illecito nell'ordinamento interno, il secondo concerne la natura stessa dell'illecito e il terzo è relativo al grado di severità della sanzione che l'interessato rischia di subire*».

[308] Le sanzioni previste possono ammontare sino a 10.000.000 euro e fino al 2% dell'intero fatturato mondiale del trasgressore, se superiore a tale importo.

tra i quali vi è anche la collaborazione con l'autorità di vigilanza, che però non ha carattere esimente, ma comporta un'eventuale diminuzione della pena; mentre, nulla viene detto in relazione al pericolo di autoincriminazione conseguente alla segnalazione. Essendo sanzioni penali il soggetto dovrebbe aver diritto alle garanzie previste per le indagini preliminari e, in particolare, al diritto al silenzio come articolazione di quello più generale di non autoaccusarsi.

Di fatto, non esiste a priori un'antinomia tra il dovere di *accountability* e il privilegio contro l'autoincriminazione, in quanto dev'essere effettuata una valutazione concreta caso per caso, considerato che la facoltà di avvalersi del diritto al silenzio spetta solo al soggetto qualificato come potenziale accusato o trasgressore. Si ritiene comunque necessario che detto diritto sia riconosciuto a livello normativo, dato che nel nostro ordinamento vi è solo l'art. 63 c.p.p.[309], che si riferisce al processo penale in senso stretto, ma estendibile anche alla fase amministrativa grazie all'art. 220 disp. att. c.p.p. L'esercizio di questa facoltà non si può considerare come condotta ostruzionistica, con la conseguenza che le eventuali sanzioni amministrative o penali irrogate, nel caso di mancata collaborazione, risultano essere illegittime.

Diverso il discorso nel caso in cui si applichino delle sanzioni disciplinari, queste per definizione non rientrano nell'art. 6 Convenzione europea dei diritti dell'uomo; dunque, si potranno applicare nonostante il soggetto abbia esercitato il diritto al silenzio, in questo caso si ritiene prevalente l'obbligo di fedeltà del segnalante all'organizzazione rispetto al suo interesse individuale; salvo casi eccezionali, in cui dette sanzioni risultino essere talmente gravi da essere qualificate come penali. Il segnalante può pur sempre godere delle tutele connesse al *whistleblowing*, per cui la denuncia di violazioni rimane una mera facoltà per cui, per definizione, il suo mancato esercizio non può essere sanzionato.

---

[309] *Ex* art. 63 c.p.p.: «*1. Se davanti all'autorità giudiziaria o alla polizia giudiziaria una persona non imputata ovvero una persona non sottoposta alle indagini rende dichiarazioni dalle quali emergono indizi di reità a suo carico, l'autorità procedente ne interrompe l'esame, avvertendola che a seguito di tali dichiarazioni potranno essere svolte indagini nei suoi confronti e la invita a nominare un difensore. Le precedenti dichiarazioni non possono essere utilizzate contro la persona che le ha rese. 2. Se la persona doveva essere sentita sin dall'inizio in qualità di imputato o di persona sottoposta alle indagini, le sue dichiarazioni non possono essere utilizzate*».

Prendendo in considerazione un'azienda si può notare come il riconoscimento del diritto al silenzio ad una persona giuridica risulti essere particolarmente problematico, soprattutto qualora disponga di un'organizzazione complessa. Vi è chi non riconosce suddetto diritto in capo all'ente, perché ritenuto una prerogativa esclusiva delle persone fisiche, di conseguenza l'ente non potrà godere degli stessi diritti di una persona fisica nel processo. Le garanzie processuali di cui un ente può godere, secondo quanto disposto agli artt. 34 e 35 del D. Lgs. 231/2001[310], prevedono i diritti e le facoltà riconosciuti ad un imputato persona fisica, in quanto compatibili. A livello sovranazionale la Corte europea dei diritti dell'uomo riconosce la protezione dei diritti umani anche per le persone giuridiche, legittimate a ricorrere alla Corte di Strasburgo, non essendoci differenze *ratione personae* che troverebbero adeguata giustificazione sotto il profilo della parità di trattamento.

Dato che la conoscenza dell'informazione autoincriminante è nell'esclusiva sfera di dominio del soggetto che si avvale della facoltà di non rispondere, l'ente non potrà che assumere lo stesso contegno. Vi possono essere due conclusioni opposte. Da un lato, è sempre legittima la sanzione per omessa collaborazione perché l'ente subisce un danno dal silenzio, dimostrando una cointeressenza per immedesimazione con le ragioni dell'imputato. Dall'altro lato, l'ente impossibilitato a dissociarsi, non può che subire le scelte del membro interno dell'organizzazione. In tal modo l'ente non potrebbe essere punito, non essendo nel suo dominio la scelta di non cooperare, diversamente si riconoscerebbe all'ente una responsabilità oggettiva per fatto altrui.

Si potrebbero verificare delle situazioni intermedie, nelle quali l'ente, prevedendo dei meccanismi sussidiari di controllo aziendale e flussi di informazioni, consentirebbe a soggetti diversi, rispetto a quello preposto alla specifica funzione aziendale, di effettuare un *self reporting* con lo scopo di far emergere fatti illeciti. In questo caso, potrebbe sorgere un conflitto tra dovere di fedeltà o lealtà del datore di lavoro (ente nel suo complesso) nei

[310] *Ex* art. 34 del D. Lgs. 231/2001: «*Per il procedimento relativo agli illeciti amministrativi dipendenti da reato, si osservano le norme di questo capo nonché, in quanto compatibili, le disposizioni del Codice di procedura penale e del decreto legislativo 28 luglio 1989, n. 271*». *Ex* art. 35 del D. Lgs. 231/2001: «*All'ente si applicano le disposizioni processuali relative all'imputato, in quanto compatibili*».

confronti dei colleghi e il dovere diffuso di controllo di legalità dell'organizzazione stessa. È evidente che, finché non sono previste disposizioni premiali, l'ente non sarà incentivato a collaborare con l'autorità amministrativa, dissociandosi dal comportamento individuale, non essendo una scelta conveniente.

L'adozione di meccanismi premiali e l'esaltazione del ruolo proattivo dell'ente potrebbe rendere superflua un'analisi dell'attribuzione del privilegio contro l'autoincriminazione, tematica che rimarrebbe isolata al solo individuo operante al suo interno, senza che ciò limiti l'efficacia del controllo diffuso, che verrebbe garantito da iniziative dell'ente stesso, sempre nei limiti in cui ciò sia materialmente possibile in base alla sua organizzazione complessiva[311].

### 4.4. *La colpa organizzativa e il principio dell'*accountability

Si evidenzia come entrambe le normative spingano sinergicamente verso una sempre crescente responsabilizzazione delle strutture aziendali. Il presupposto del regime sanzionatorio *ex* D. Lgs. 231/2001 è quello della responsabilità colposa per mancata predisposizione delle misure necessarie ad impedire la commissione di reati nell'interesse o in vantaggio dell'azienda, da parte di soggetti interni ad essa. Mentre, uno dei pilastri del GDPR è il principio dell'*accountability*, assimilabile al principio di responsabilità che comprende aspetti quali l'affidabilità e la competenza aziendale nella gestione dei dati personali. Il principio di *accountability* è recepito all'art. 24 del GDPR il quale prevede che tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al Regolamento.

[311] cit. A. FABERI, op. cit., p. 27. Riassumendo il concetto appena esposto: secondo l'autore, *de iure condendo*, lo scollamento tra il dovere di "*cooperation*" e la punibilità in caso di "*self-reporting*" potrà essere colmato solo con un pronunciato aumento delle condizioni premiali per l'ente stesso.

Quindi, tra le normative vi è un punto di contatto, caratterizzato dalla responsabilizzazione delle aziende. Si richiede di organizzare la realtà aziendale in modo da predisporre misure tecniche ed organizzative idonee ad impedire la commissione di reati presupposto e la commissione di violazioni nel trattamento dei dati personali.

È chiaro come entrambi questi istituti affianchino ad un profilo meramente giuridico una dimensione etica che incentiva un decisionismo responsabile in grado di promuovere un dialogo rispettoso della legalità. Si impongono come strumenti per l'attuazione di meccanismi pratici in un contesto in cui l'adempimento degli obblighi legali e la garanzia di un'assistenza adeguata diventano indici virtuosi della tutela dei dati e della salvaguardia dalla commissione di reati.

### 4.5. *Prospettiva* de iure condendo*: il problema del* ne bis in idem *sostanziale*

La coesistenza del D. Lgs. 231/2001 e del Regolamento (UE) 2016/679 potrebbe creare una difficoltà ulteriore da dover necessariamente affrontare. L'applicazione delle suddette due normative, visto l'inscindibile collegamento che sussiste tra i reati informatici e la tutela della riservatezza, potrebbe creare un doppio binario sanzionatorio, caratterizzato da sanzioni amministrative e sanzioni penali, lesivo del principio del *ne bis in idem* sostanziale[312].

Con riferimento alla responsabilità amministrativa degli enti, tale problema potrebbe porsi nell'ipotesi in cui le fattispecie *privacy* diventassero anche reato presupposto ai sensi del D. Lgs. 231/2001, dato che ad oggi, come già analizzato non vi rientrano gli artt. 167 e ss. del Codice *privacy*, nonostante la loro connessione con gli altri reati informatici inseriti nel catalogo. Ferma la necessità di un intervento legislativo, di ampio respiro che non sia unicamente volto a editare l'elenco dei reati presupposto, con la solita tecnica legislativa del "taglia e cuci", ma che sia invece funzionale ad introdurre

[312] Per quanto attiene al concetto di *ne bis in idem* sostanziale vd. nota 197.

una vera e propria disciplina organica della materia *de quo*, potrebbe effettivamente ammettersi una sanzione penale accanto a quella amministrativa[313].

Qualora le violazioni corrispondano a fattispecie di *cybercrimes* previste dal Codice penale, ovvero a ipotesi di trattamento illecito di dati, l'Autorità garante per la protezione dei dati personali potrebbe comminare una sanzione amministrativa ai sensi dell'art. 83 del GDPR e contemporaneamente per le medesime violazioni si applicheranno anche le sanzioni penali previste dal Decreto 231 addebitando, in tal modo, più volte lo stesso fatto al medesimo soggetto.

Si delinea un sistema sanzionatorio basato sul c.d. doppio binario; con questa espressione, ci si riferisce all'applicazione congiunta di sanzioni penali e amministrative per un medesimo fatto. Tale tecnica punitiva, nell'ambito del diritto italiano, non incontra ostacoli, in quanto l'art. 649 c.p.p. vieta il *bis in idem* solo con riguardo alle sanzioni penali. Tuttavia, la giurisprudenza della Corte europea dei diritti dell'uomo, a partire dalla sentenza dell'8 giugno 1976, *Engel* c. *Paesi Bassi*, ha elaborato una serie di indici volti a riqualificare la sanzione formalmente amministrativa, secondo il diritto interno, per attribuirle natura sostanzialmente penale. La natura intrinsecamente penale determina l'applicazione delle garanzie convenzionali previste per la materia penale, fra cui il divieto di *bis in idem*, sancito dall'art. 4, prot. VII, Convenzione europea per la salvaguardia dei diritti dell'uomo[314].

Nei sistemi basati sul doppio binario il concorso apparente[315], della norma penale con quella amministrativa, che condurrebbe all'applicazione di due sanzioni sostanzialmente penali, viene risolto attraverso l'applicazione del principio di specialità di cui all'art. 15 del codice penale secondo il quale «*lex specialis derogat generali*»[316].

---

[313] cit. P. BALBONI, F. TUGNOLI, op. cit., p. 16.

[314] cit. P. SALVEMINI, *Il doppio binario sanzionatorio al vaglio della Corte di Giustizia: la Grande Sezione si pronuncia sulle questioni pregiudiziali*, in *dirittticomparati.it*, 2018.

[315] Il concorso apparente di norme si verifica quando una medesima condotta pare riconducibile a più precetti penali, ciascuno dei quali esaurisce il disvalore del fatto. Per capire quale norma applicare qualora si verifichi un concorso apparente la giurisprudenza e la dottrina hanno elaborato diversi criteri che tuttavia sono stati ricondotti esclusivamente al principio di specialità da parte delle Sezioni Unite (cfr. Cass pen., sez. un., 22 giugno 2017, n. 41588, sent.).

[316] Secondo il principio *lex specialis derogat generali* si applicherà la legge speciale che andrà a

Per comprendere quale sia la norma speciale la giurisprudenza individua alcuni criteri[317]; il principale, è quello che fa leva sulla nozione di medesimo fatto inteso quale medesima presunta violazione. Per capire se due pronunce abbiano ad oggetto un medesimo fatto è necessario verificare l'identità concreta e materiale dei fatti e non la condotta come descritta dalle norme[318], andando oltre al profilo meramente descrittivo delle norme penale e amministrativa. Dunque, bisognerebbe verificare se, il fatto oggetto della sanzione amministrativa comminata dal Garante sia il medesimo che possa dare origine ad una sanzione penale. Per concludere, per norma speciale si intende quella norma che contiene tutti gli elementi compresi nella fattispecie generale, più ulteriori elementi specifici; tra le due norme deve esistere un rapporto tale che, se mancasse la norma speciale, la fattispecie sarebbe ricompresa nella norma generale.

La sanzione penale ai sensi dell'art. 24-*bis* del Decreto 231 può ritenersi violativa del principio del *ne bis in idem* sostanziale nella misura in cui, secondo i criteri ermeneutici elaborati dalla giurisprudenza, il fatto materiale, verificatosi nella realtà concreta che da origine alla sanzione penale e amministrativa, sia il medesimo.

In conclusione, qualora vi fosse un'eventuale riforma della responsabilità amministrativa degli enti, per cui vengono chiamati a rispondere delle violazioni penali *privacy* ai sensi degli artt. 167 e ss. del Codice *privacy*, per superare l'*empasse* del *ne bis in idem* sostanziale, dovrebbe ritenersi che la responsabilità penale derivante dal Codice *privacy* si limiti ai soli titolari del trattamento persone fisiche, mentre, per tutti gli altri soggetti si prevede solo la responsabilità *ex* Decreto 231.

---

derogare la legge generale, quest'ultima vede il suo ambito di applicazione ristretto ai casi in cui non trova applicazione la legge speciale. L'art. 15 c.p. recita: «*Quando più leggi penali o più disposizioni della medesima legge penale regolano la stessa materia, la legge o la disposizione di legge speciale deroga alla legge o alla disposizione di legge generale, salvo che sia altrimenti stabilito*».

[317] vd. Cass pen., sez. un., 22 giugno 2017, n. 41588, sent.

[318] vd. Corte EDU, 10 febbraio 2015, C-53753/12, *Kiiveri* c. *Finlandia*.

### 4.6. *Il* whistleblowing *tra GDPR e D. Lgs. 231/2001*

La disciplina del *whistleblowing*[319], inteso quale strumento di *compliance* aziendale, con il quale i dipendenti oppure terze parti di un'azienda possono segnalare, in modo riservato e protetto, eventuali illeciti riscontrati durante la propria attività, fa ingresso nel nostro ordinamento nel 2017 con la Legge n. 179 e prevede una tutela specifica per i soggetti che segnalino reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro. La regolamentazione nel settore privato inizialmente era contenuta all'art. 6, nei commi 2-*bis*, 2-*ter* e 2-*quater* del D. Lgs. 231/2001, introdotti dalla suddetta Legge, i quali successivamente sono stati abrogati dall'art. 23 del D. Lgs. n. 24 del 10 marzo 2023[320]. Infine, la Direttiva (UE) 1937/2019, c.d. Direttiva *whistleblowing*, e il successivo D. Lgs. 24/2023, hanno riformato la materia con l'obiettivo di rafforzare i principi di trasparenza e responsabilità e prevenire la commissione di reati, senza distinzione tra settore pubblico e privato.

La tutela prevede tre direttici: divieto di discriminazioni; riservatezza dell'identità del segnalante; sanzioni disciplinari per chi viola le misure di tutela o chi presenta, con dolo o colpa grave, segnalazioni che si rivelino infondate[321].

Si noti come detta disciplina abbia delle interconnessioni sia con il GDPR che con il Decreto 231 e quindi ne rappresenti un punto di contatto.

Qualora vi sia una segnalazione si creano diversi soggetti interessati, ossia soggetti i cui dati sono trattati da parte del titolare nella procedura di *whistleblowing*. I soggetti interessati sono il segnalante, il segnalato ed eventuali terzi a cui si fa riferimento,

---

[319] vd. nota 268.

[320] Decreto di "*Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali*".

[321] L'art. 6 del D. Lgs. 231/2001 prevede che sia sanzionato, oltre al soggetto che abbia posto in essere problemi di ritorsione o discriminatori nei confronti del *whistleblower*, anche colui che «*effettua con dolo o colpa grave segnalazioni che si rivelano infondate*». Occorre un impianto sanzionatorio *ad hoc* per questi ipotesi da integrare nel sistema disciplinare *ex* art. 6, comma 2, lett. e), del Decreto 231/01. Nell'espletamento dell'attività di vigilanza, particolare attenzione dovrà essere posta dall'OdV su licenziamenti o altre misure (*e.g.* demansionamenti e trasferimenti) che possano avere natura ritorsiva o discriminatoria nei confronti del segnalante (cit. M. CIRIGLIANO, op. cit., nota 11).

direttamente o indirettamente, all'interno della segnalazione. L'acquisizione e la gestione delle segnalazioni dà luogo a trattamenti di dati personali, anche appartenenti a particolari categorie di dati e relativi a condanne penali e reati; per questo motivo è oggetto di attenzione da parte del Garante *privacy*. L'impresa che predispone un protocollo di *whistleblowing* è titolare del trattamento, ovverosia il soggetto che determina le finalità e i mezzi del trattamento dei dati personali[322]. Gli enti pubblici o privati, essendo titolari del trattamento, dovranno tenere in considerazione, nell'ambito delle proprie scelte organizzative, finalizzate all'istituzione e gestione di propri canali di segnalazione[323], una serie di principi di carattere generale e rimanere coerenti con i principi di responsabilizzazione e di protezione dei dati fin dalla progettazione e per impostazione predefinita, nonché con i principi di integrità e riservatezza dei dati. Quindi, la procedura in esame dovrà avvenire nel pieno rispetto della normativa in materia di protezione dei dati personali, garantendo, in pari tempo, il necessario bilanciamento tra esigenza di riservatezza della segnalazione, necessità di accertamento degli illeciti e diritto di difesa e di contraddittorio del segnalato, considerati altresì i rischi per gli interessati nel delicato contesto lavorativo e professionale[324].

Vi è un'intersezione tra la disciplina in materia di *whistleblowing* e il Modello Organizzativo *Privacy*. Anzitutto, la segnalazione dev'essere formulata in maniera tale da contenere ogni elemento utile al fine di favorire le verifiche necessarie per dare riscontro oggettivo ai fatti segnalati[325]. Le segnalazioni prese in considerazione sono solo quelle che presentano elementi adeguatamente circostanziati, relativi a fatti di particolare gravità.

Nel trattamento di dette segnalazioni si potranno delineare delle difficoltà nella

---

[322] *Ex* art. 4, n. 7 del GDPR.

[323] Il canale di segnalazione può essere interno, nell'ambito del contesto lavorativo ovvero esterno, gestito direttamente dall'Autorità Nazionale Anticorruzione (ANAC).

[324] cit. Garante per la Protezione dei Dati Personali, parere n. 304, *Schema di Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali – procedure per la presentazione e gestione delle segnalazioni esterne*, 6 luglio 2023, p. 6.

[325] Per tale motivo dovranno essere riportati: identificazione delle persone coinvolte (segnalante, segnalati e altre persone coinvolte); fatti segnalati, elementi raccolti nella verifica; rendiconto delle operazioni di verifica; ed infine, epilogo della segnalazione.

conciliazione con la protezione dei dati personali, soprattutto nella fase di indagine, di raccolta informazioni e di valutazione sia preliminare che successiva, nella quale si accerta la veridicità. In questa fase entra in gioco la figura del Responsabile della gestione dei canali di segnalazione, il quale condurrà le indagini con imparzialità e riservatezza, effettuando ogni attività idonea ad approfondire la fondatezza o meno della segnalazione.

In conclusione, l'organizzazione dovrà prevedere una procedura che gestisca, nel rispetto della menzionata Legge: i diritti del segnalante e del segnalato, nonché degli eventuali terzi coinvolti; i tempi, i luoghi di conservazione della documentazione, sia che questa abbia dato adito a provvedimenti o meno, e le relative modalità di accesso; l'informativa agli interessati identificando il trattamento, tanto nel ruolo di segnalante quanto di segnalato[326]. Inoltre, verrà predisposto un regolamento contenete: misure idonee a garantire l'anonimato del segnalate; modalità per distruggere i dati trattati; registro dei trattamenti contenente il trattamento in questione; analisi dei rischi e DPIA, dato che si tratta di un trattamento ad elevato rischio per i diritti e le libertà fondamentali degli interessati; indicazione dei soggetti autorizzati al trattamento dei dati; i contratti con i responsabili ed eventuali contitolari, nel caso di gestione con altri soggetti; ed infine, i tempi di conservazione dei dati, decorsi i quali dovranno essere cancellati[327].

Vige il principio di minimizzazione, per cui i dati che il titolare è legittimato a raccogliere durante la procedura di segnalazione, sono solo quelli necessari e utili per il raggiungimento della finalità perseguita.

La Legge n. 179/2017 con riguardo al settore privato, aveva imposto solo alle organizzazioni che, volontariamente, avessero scelto di adottare i Modelli organizzativi 231, l'obbligo di implementare canali di segnalazione e di garantire una protezione contro eventuali atti ritorsivi nei confronti di chi avesse fatto emergere violazioni dei Modelli o condotte illecite integranti i reati presupposto.

---

[326] cit. C. E. PONTI, S. PERSI, M. A. PEREGO, op. cit., pp. 60 ss.

[327] A tal proposito, merita di essere ricordato il protocollo "HTTPS", acronimo di *Hyper Text Transfer Protocol Secure*, sfruttando avanzati sistemi di crittografia, cifra la comunicazione tra *server* e utente finale proteggendo il contenuto del messaggio e poi la rete TOR (acronimo di *The Onion Router*), che avvolge i dati con una cifratura a strati multipli assicurando l'anonimato del segnalante, rendendo impossibile per il destinatario e per tutti gli intermediari nella trasmissione avere traccia dell'indirizzo *internet* del mittente (cit. M. CIRIGLIANO, op. cit., p. 8).

Questo binomio tra *compliance* 231 e *whistleblowing* è stato in parte superato dal nuovo D. Lgs. 24/2023. Detto Decreto amplia il concetto di *whistleblower* e, in particolare, non circoscrive più l'applicazione dell'istituto ai soli enti dotati di un Modello organizzativo e alle sole segnalazioni relative ad illeciti o violazioni rilevanti per la responsabilità *ex* Decreto 231. Il D. Lgs. 24/2023 estende l'obbligo di attivare un sistema per segnalare violazioni del diritto nazionale e dell'Unione Europea a tutti gli enti privati che soddisfano almeno una delle seguenti condizioni: nell'ultimo anno, abbiano impiegato la media di almeno cinquanta lavoratori subordinati con contratti di lavoro a tempo indeterminato o determinato, a prescindere dal settore di appartenenza; si occupano di alcuni settori specifici, ad esempio: servizi, prodotti e mercati finanziari; adottano un MOGC, anche se nell'ultimo anno non hanno raggiunto la media di almeno cinquanta lavoratori subordinati con contratti di lavoro a tempo indeterminato o determinato. Infine, stabilisce un periodo di tempo entro il quale gli enti dovranno adeguarsi e qualora questi non lo facciano saranno destinatari di sanzioni amministrative pecuniarie.

Con la nuova disciplina, quindi, ogni impresa operante in Italia e rientrante nelle categorie appena menzionate dovrà: istituire canali per consentire segnalazioni in forma scritta, anche con modalità informatiche, oppure in forma orale; affidare la gestione dei canali di segnalazione ad una persona o ad un ufficio interno autonomo, dedicato e con personale specificamente formato, o ad un soggetto esterno, anch'esso autonomo e specificamente formato[328]; adottare una procedura per regolamentare in modo preciso la gestione delle segnalazioni, con tempistiche certe e l'obbligo di dare un seguito alle segnalazioni stesse, valutando la veridicità e la sussistenza dei fatti riportati e adottando le necessarie azioni correttive; mettere a disposizione dei possibili segnalanti informazioni chiare sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni interne o esterne o le divulgazioni pubbliche; garantire misure di tutela per

[328]In merito, nasce l'esigenza di svolgere una profonda riflessione sull'identificazione del soggetto o dell'ufficio (interno o esterno) in possesso delle dovute competenze, anche tecniche, per la gestione delle segnalazioni, essendo l'attività dell'Organismo di Vigilanza tipicamente circoscritta alle violazioni rilevanti per il Decreto 231. E, in ogni caso, si dovranno regolamentare i flussi informativi tra l'OdV e le altre funzioni aziendali (ad es. risorse umane, legale, *compliance*) che potranno essere coinvolte nelle indagini interne sulle segnalazioni, al fine di garantire la riservatezza del segnalante e delle altre persone coinvolte.

i segnalanti, consistenti in particolare nella riservatezza della loro identità, con l'esecuzione dei necessari adempimenti in materia di *data protection* e *cybersecurity,* e nel divieto di ritorsioni dirette o indirette nei loro confronti.

Se molte delle imprese ora coinvolte nella disciplina del *whistleblowing* si troveranno a dover pensare *ex novo* ai propri sistemi di segnalazione quelle che, avendo adottato i MOGC avevano anche già attivato dei canali di segnalazione, dovranno invece adeguare detti canali e, soprattutto, le relative procedure di gestione delle segnalazioni, al nuovo dettato normativo[329].

In relazione a questo argomento si riscontra un'intersezione tra i due organi preposti al controllo secondo le due normative, l'Organismo di Vigilanza e il *Data Protection Officer*; si aprono delle frontiere di vigilanza integrata che verranno analizzate ulteriormente al paragrafo successivo.

Relativamente alla procedura di *whistleblowing* l'OdV in concorso con il DPO valuteranno l'adeguatezza della procedura e vigileranno sul corretto corso delle indagini difensive interne.

L'OdV agisce affinché i segnalanti siano tutelati nel processo di gestione della segnalazione, rimanendo protagonista nella vigilanza sul rispetto del divieto di «*atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione*» come previsto all'art. 6, comma 2-*bis*, lett. c) del D. Lgs. 231/2001.

Il DPO dovrà supervisionare l'attività del titolare del trattamento e in tale veste dovrà vigilare sull' attribuzione delle responsabilità, sulla sensibilizzazione e sulla formazione del personale oltre ad effettuare assieme all'OdV le relative attività di controllo sul corretto svolgimento delle investigazioni difensive condotte dall'azienda[330].

Quindi, la procedura di *whistleblowing* è un argomento centrale per le aziende che riguarda sia il D. Lgs. 231/2001, sia il GDPR. A tal proposito, si delinea la possibilità di creare un protocollo di *whistleblowing* con ragionamenti di *compliance* integrata.

---

[329] cfr. M. H. SCHETTINO, *Compliance 231 e whistleblowing: ecco le novità*, 2023, in *Il Sole 24 Ore*.

[330] cit. M. CIRIGLIANO, op. cit., p. 9.

### 4.7. *Organi di sorveglianza a confronto:* Data Protection Officer *e Organismo di Vigilanza*

Ulteriori corrispondenze emergono sul versante degli organismi di controllo previsti dal D. Lgs. 231/2001 e dal Regolamento (UE) 2016/679, che sono, rispettivamente, l'Organismo di Vigilanza (OdV) e il *Data Protection Officer* (DPO). Questi soggetti rappresentano centri di imputazione di compiti di vigilanza, necessari affinché gli strumenti di *compliance* siano adottati ed efficacemente implementati. Entrambi svolgono controlli interni, per cui, secondo alcuni[331], potrebbe risultare conveniente un approccio multidisciplinare, così da evitare controlli diversificati tra loro che appesantiscono gli apparati organizzativi con inutili duplicazioni e un maggiore impego di risorse.

Riassumendo detti ruoli, in precedenza già analizzati[332], il DPO è strutturale rispetto all'azienda, anche se scelto fra soggetti esterni; una volta ricoperto detto ruolo, diventa parte integrante dell'azienda e concorre nella definizione delle strategie interagendo direttamente con il vertice aziendale, al quale offre, se richiesta, una consulenza sulla decisione, stante le sue ampie competenze e conoscenze professionali in ambito di protezione dei dati. Il titolare del trattamento non è vincolato a quanto consigliato dal DPO, può decidere diversamente, ma dandone un'adeguata motivazione. Il DPO è parte integrante dell'azienda perché deve poter vedere da vicino come si applicano le scelte sul trattamento dei dati personali e sui problemi operativi che queste possono comportare.

L'OdV è preposto al controllo sul funzionamento e il rispetto del MOGC[333] e, come per il DPO, deve «*essere dotato di autonomi poteri di iniziativa e controllo*» e «*deve sempre essere garantita l'autonomia dell'iniziativa di controllo da ogni forma di interferenza o di condizionamento*»[334]. L'OdV non partecipa alle scelte aziendali, riveste

[331] In tal senso *ibidem* pp. 11 e 12.
[332] vd. par. 2.4.4 e 3.4.2.
[333] *Ex* art. 6 del D. Lgs. 231/2001.
[334] Cass. pen., sez. un., n. 38343, 18 settembre 2014, sent.

un ruolo di controllo *ex post* con il quale accerta la conformità alle norme, l'efficacia esimente e la concreta attuazione del Modello organizzativo. Difficilmente i ruoli di OdV e DPO potrebbero essere rivestiti contemporaneamente da un medesimo soggetto, senza che le informazioni acquisite in relazione ad un ruolo non influenzino le decisioni assunte nell'altro ruolo.

Queste due figure nel sistema dei controlli interni condividono caratteristiche di terzietà e indipendenza ed operano un controllo di legalità sul funzionamento dell'ente. Per questo motivo, si potrebbe pensare di poterle cumulare in un unico soggetto. D'altra parte, è già fatto acquisito che il Collegio sindacale, ove presente, possa svolgere anche la funzione di Organismo di Vigilanza. Sarebbe, *prima facie*, legittimo pensare di attribuire anche il ruolo di Responsabile per la Protezione dei Dati a chi già ricopre i ruoli in questione. Ci sono, tuttavia, diversi motivi che lo sconsigliano (o addirittura vietano) una scelta del genere e che, ancora una volta, dipendono dalla differenza degli obbiettivi perseguiti dalla normativa sul trattamento dei dati personali e da quella sulla responsabilità amministrativa delle imprese[335].

Entrambi questi soggetti valutano la correttezza dei processi posti in essere in adempimento delle norme delle quali ciascuno è il custode. I processi previsti dal GDPR sono orientati alla minimizzazione dei trattamenti. All'opposto, i processi ai sensi del Decreto 231 hanno l'obbiettivo di dissuadere i soggetti, parte dell'organico dell'ente, dalla commissione di reati presupposto, per cui il controllo dell'OdV dovrebbe avere la massima estensione consentita dalla legge. Quindi, si ravvisa una collisione tra il controllo svolto dall'OdV con il principio di minimizzazione previsto dal GDPR.

Si può concludere affermando che le autorità di sorveglianza non sono pienamente convergenti, sulla base di diversi motivi, tra i quali: il GDPR determina in maniera chiara e precisa i poteri e i compiti del DPO, rispetto a quanto faccia il Decreto 231 con l'OdV; la nomina dell'OdV è necessaria per soddisfare i requisiti minimi di adeguatezza del Modello organizzativo adottato dall'ente, viceversa, il DPO viene individuato solo in determinati contesti ovvero per particolari tipologie di operazioni su dati; infine,

[335] cit. L. LUPARIA [et. al.], A. MONTI (a cura di), op. cit., pp. 241 e 242.

fondamentale è la prevenzione di conflitti di interessi per cui le posizioni di DPO e OdV sono apparentemente inconciliabili.

Doveroso, stante l'assenza di pronunce giurisprudenziali e il silenzio dell'Autorità garante, un maggior approfondimento sulla relazione che intercorre tra il DPO e l'OdV, anche alla luce del requisito di indipendenza e alla necessità che il Responsabile per la Protezione dei Dati operi in assenza di conflitti di interessi[336] ai sensi dell'art. 38 del GDPR.

Per comprendere fino in fondo le differenze insanabili tra queste due figure, nel paragrafo successivo, verrà analizzata una problematica nel dettaglio: la qualificazione soggettiva dell'Organismo di Vigilanza ai fini *privacy*.

### 4.7.1. *La qualificazione soggettiva dell'Organismo di Vigilanza ai fini della* **privacy**

L'Organismo di Vigilanza, affinché possa espletare le sue funzioni di controllo di efficacia del MOGC, sembrerebbe doversi qualificare *ex lege* quantomeno come responsabile esterno, se non addirittura come titolare autonomo del trattamento dei dati personali, il che escluderebbe la possibilità di cumulare il suo ruolo con quello del *Data Protection Officer*. In realtà, alcuni autori notano che, generalmente, l'OdV non tratta i dati personali con modalità tali da essere sottoposto alle disposizioni del GDPR[337]. La verifica dell'efficacia formale del Modello 231 non prevede di per sé un trattamento di dati personali, trattandosi di un'attività meramente documentale ed astratta; vale lo stesso per i compiti di verifica dell'effettiva adozione e gestione delle segnalazioni[338].

---

[336] Per conflitto di interessi si intende quella condizione giuridica nella quale un soggetto, investito di poteri decisionali, possiede un interesse personale/professionale in contrasto con la carica per la quale gli sono stati attribuiti tali poteri (cit. C. PIVATO, *DPO e organismo di vigilanza (ODV): definire ruoli e competenze per evitare conflitti di interesse*, in *cybersecurity360.it*, 2019).

[337] cfr. L. LUPARIA [et. al.], A. MONTI (a cura di), op. cit., p. 242.

[338] A tal proposito, nel caso di piattaforme di *whistleblowing*, come il progetto *open source* chiamato *Globaleaks* che ha l'obbiettivo di tutelare l'identità del segnalante, l'OdV potrebbe conoscere il fatto, ma non necessariamente l'identità del segnalato.

Di converso, qualora si ritenga che detto organo, nell'esercizio delle sue funzioni, attui un trattamento di dati, per cui dovrà essere sottoposto alla disciplina contenuta nel GDPR, si presentano una serie di dubbi circa la sua qualificazione soggettiva ai fini *privacy*. Con nota del 16 ottobre 2019 l'Associazione dei Componenti degli Organismi di Vigilanza *ex* D. Lgs. 231/2001[339] richiese al Garante per la *privacy* un incontro, nel corso del quale l'Associazione espose la propria posizione in merito con un *Position Paper*, approvato dal Consiglio Direttivo il 21 marzo 2019, e il Garante espresse la sua opinione in un Parere datato 12 maggio 2020. Entrambi i punti di vista verranno analizzati nei paragrafi successivi.

#### 4.7.1.1. *Il* Position Paper *dell'Associazione degli Organismi di Vigilanza* ex *D. Lgs. 231/2001*

In seguito, verranno ripercorse le tappe fondamentali affrontante dall'AODV231 nel *Position Paper*. Partendo dall'origine del problema, si ritiene che l'OdV nello svolgimento delle sue attività entra inevitabilmente in contatto con dati personali, in particolare con dati sensibili e giudiziari[340]. Questi dati derivano da una serie di fonti che riguardano l'Organismo: i flussi informativi *ex* art. 6, comma 2, lett. d) del D. Lgs. 231/2001; i risultati delle attività di controllo e vigilanza *ex* art. 6, comma 1, lett. b) e d) del D. Lgs. 231/2001; infine, eventualmente e non necessariamente[341], le segnalazioni di condotte illecite rilevanti o di violazioni del Modello *ex* art. 6, comma 2-*bis*, lett. a) del D. Lgs. 231/2001.

Il tema inizialmente si polarizzava tra due soluzioni opposte, senza alternativa,

[339] Detta anche "AODV231" è l'Associazione senza fini di lucro che riunisce professionisti e esponenti aziendali che vivono in prima persona l'esperienza degli Organismi di Vigilanza previsti dai Modelli di Organizzazione adottati in base al D. Lgs. 231/2001.

[340] Disciplinati dall'art. 9 del GDPR, rubricato "Trattamento di categorie particolari di dati personali".

[341] Il riferimento all'OdV dei canali di *whistleblowing* costituisce una scelta aziendale discrezionale, da valutare attentamente per i suoi possibili riflessi sul regime della responsabilità dell'Organismo e sulla sua qualificazione soggettiva secondo la disciplina di protezione dei dati personali.

che davano per scontata l'autonoma soggettività *privacy* dell'OdV rispetto all'ente vigilato. Quindi, la questione era: se all'Organismo di Vigilanza si dovesse attribuire il ruolo di titolare ovvero di responsabile del trattamento dei dati personali.

L'unica variante recente sembra quella di declinare la vecchia alternativa, ora in riferimento all'OdV come organismo collegiale ora, addirittura, in riferimento ai singoli membri dell'OdV, distinguendo tra "membri interni", per così dire già "coperti" dall'inquadramento *privacy* predeterminato dal rapporto di lavoro subordinato con l'ente vigilato, e "membri esterni", per i quali soltanto si proporrebbe la tralaticia alternativa qualificatoria titolare/responsabile[342].

Il lavoro svolto nel *Postition Paper* dall'Associazione prevede un'analisi critica delle tesi correnti e arriva a delineare un'alternativa secondo la quale l'Organismo non è né titolare né responsabile, ed il suo inquadramento soggettivo ai fini della *privacy* è assorbito da quello della società vigilata della quale, appunto, l'OdV è parte. Detta tesi si basa su diversi assunti: l'Organismo ha un carattere essenzialmente interno rispetto all'ente, implicato dall'art. 6, comma 1, lett. b) del D. Lgs. 231/2001 laddove si riferisce «*a un organismo dell'ente*», per cui vi è questo requisito di appartenenza all'ente[343]; le nozioni di titolare e responsabile del trattamento sono autonome, devono interpretarsi secondo quanto disposto dalle disposizioni comunitarie relative alla protezione dei dati; il carattere funzionale ed imperativo della nozione di titolare fa intendere che il ruolo rivestito dipende concretamente dall'effettivo potere decisorio esercitato, a prescindere

[342] cit. Associazione dei Componenti degli Organismi di Vigilanza *ex* D. Lgs. 231/2001, *Sulla qualificazione soggettiva dell'Organismo di Vigilanza ai fini privacy*, Milano, 2019,4.

[343] Detto requisito di appartenenza dell'Organismo di Vigilanza all'ente è pressoché pacificamente riconosciuto dalla dottrina (cfr. C. SANTORIELLO, *Attività dell'organismo di vigilanza e obbligo di segretezza in capo ai suoi componenti*, in *La responsabilità amministrativa delle società e degli enti*, 2015, 4, pp. 109 ss.; N. PISANI, *I requisiti di autonomia ed indipendenza dell'organismo di vigilanza istituito ai sensi del d. lgs. 231/2001*, in *La responsabilità amministrativa delle società e degli enti*, 2015, 1, pp. 155 ss.) dalla giurisprudenza (cfr. Trib. Milano, 20 settembre 2004, n. 30.382-03, ord.) e dalle Linee Guida di categoria (cfr. ASSOCIAZIONE BANCARIA ITALIANA, *Linee guida dell'Associazione Bancaria Italiana per l'adozione di modelli organizzativi sulla responsabilità amministrativa delle banche*, 2004, p. 21; CONFINDUSTRIA, *Linee Guida per la costruzione di modelli di organizzazione, gestione e controllo*, 2022, p. 20).

da eventuali diverse qualificazioni formali, ad esempio ruoli decisi pattiziamente in un contratto[344].

In passato sotto il vigore del "vecchio" Codice della *privacy* si riteneva che la funzione del responsabile potesse essere attribuita dal titolare anche a persone, organi o strutture interne alla sua organizzazione, con effetti esterni verso l'Autorità di controllo e gli interessati. Secondo quanto disposto dall'art. 4, lett. f) il responsabile era definito quale persona fisica, giuridica, qualsiasi altro ente o organismo «*preposti dal titolare al trattamento di dati personali*». Con l'entrata in vigore del GDPR e l'abrogazione dell'art. 4 del D. Lgs. 196/2003 ad opera dell'art. 27, comma 1, lett. a), n.1 del D. Lgs. 101/2018[345], detta possibilità è venuta meno, escludendosi la figura del "responsabile interno"[346].

L'Organismo di Vigilanza secondo quando previsto dal Decreto 231 può essere un organo monocratico ovvero collegiale; data la necessità di disporre di diverse professionalità si predilige, soprattutto in relazione ad entità complesse e di grandi dimensioni, il ricorso alla struttura collegiale. A tal proposito, ci si domanda se l'OdV, in quanto organismo collegiale, debba essere complessivamente considerato ovvero debba essere considerato singolarmente ciascun membro che ne faccia parte. L'art. 28 del D. Lgs. 196/2003 risponde a questa domanda, per cui le qualifiche soggettive ai fini *privacy* di soggetti articolati devono riferirsi all'entità nel suo complesso, considerando come responsabile del trattamento la società o l'organismo in quanto tali, piuttosto che una specifica persona al loro interno[347]. Quindi, quale che sia la qualificazione soggettiva ai fini della normativa sulla *privacy*, questa si deve riferire all'OdV nel suo complesso, come organismo collegiale e non a ciascun membro singolarmente.

---

[344] cfr. L. BOLOGNINI, E. PELINO, C. *BI*STOLFI, *Il regolamento privacy europeo*, Milano, 2016, pp. 121 e 131.

[345] La Relazione illustrative del D. Lgs. 101/2018 precisa che «*l'*art. *2-quaterdecies, rubricato «Attribuzione di funzioni e compiti a soggetti designati», prevede il potere di Titolare e Responsabile, di delegare compiti e funzioni a persone fisiche che operano sotto la loro autorità e che, a tale fine, dovranno essere espressamente designati. Tale disposizione permette di mantenere le funzioni e i compiti assegnati a figure interne all'organizzazione che, ai sensi del previgente codice in materia di protezione dei dati ma in contrasto con il regolamento, potevano essere definiti, a seconda dei casi, Responsabili o Incaricati*».

[346] Per essere chiari la figura di responsabile interno può continuare a sussistere giuridicamente attraverso l'istituto giuridico della procura speciale.

[347] cit. WP29, op. 1/2010, par. III.1.c.

Come prima detto, inizialmente si delinearono due tesi contrapposte che qui di seguito verranno analizzate con sguardo critico.

Secondo una parte della dottrina, l'Organismo di Vigilanza sarebbe qualificabile come titolare del trattamento, sulla base dell'assioma che si crea tra gli «*autonomi poteri di iniziativa e controllo*», propri dell'Organismo, e i poteri di «*determinare le finalità e i mezzi del trattamento dei dati personali*», propri del titolare. Il requisito di autonomia caratterizza lo spettro di funzioni esercitabili dall'OdV e non le attività necessarie all'espletamento di dette funzioni, tra le quali vi è il trattamento dei dati. In particolare, le finalità del trattamento non sono determinate dall'Organismo stesso, ma sono predeterminate dalla legge e declinate al Modello 231 da parte dell'Organo dirigente; infine, lo stesso OdV viene istituito dall'Organo dirigente che ne disciplina gli aspetti principali. Mentre, per quanto riguarda i mezzi, questi potranno essere codeterminati dall'OdV insieme all'Organo dirigente, poiché si tratta di questioni sia tecniche che organizzative, la cui decisione può essere delegata.

La funzione di determinare le finalità del trattamento fa scattare automaticamente la qualifica di titolare del trattamento; viceversa, la determinazione dei mezzi fa scattare la titolarità solo qualora riguardi i loro aspetti fondamentali, cosa che normalmente non accade per l'OdV perché, detti elementi fondamentali, sono riconducibili a quelli relativi al suo funzionamento che vengono disciplinati dall'Organo dirigente.

L'autonomia dell'Organismo di Vigilanza, che si riferisce al suo compito di vigilare, è da tenere ben distinta dall'autonomia nella determinazione delle finalità di vigilanza e quindi dei trattamenti strumentali ad essa. Anche se l'OdV non venisse qualificato come titolare vi sarebbe ugualmente la tutela della sua autonomia *ex* art. 28, comma 3, lett. a) e lett. h) del GDPR. Le Linee Guida Confindustria precisano che «*L'OdV riveste una posizione autonoma e imparziale, prevedendo il "riporto" al massimo vertice operativo aziendale, vale a dire al Consiglio di Amministrazione*»[348]. Infine, occorre ricordare che il rispetto delle norme al cui controllo l'Organismo di Vigilanza è preposto è, prima di tutto, un obbligo gravante sulla società oggetto del controllo, per cui

[348] cit. CONFINDUSTRIA, op. cit., p. 77.

quest'organo è uno strumento attivato per legge; sicché i dati oggetto dei loro trattamenti sono quelli che l'ente controllato ha diritto e legittimazione a trattare, già appartenenti all'azienda, senza bisogno che l'OdV ne raccolga di nuovi.

L'Organismo di Vigilanza non può essere considerato quale titolare del trattamento ai sensi dell'art. 4, n. 7), primo periodo del GDPR. Il concetto di titolare del trattamento è autonomo e funzionale, ovverosia finalizzato all'assegnazione di responsabilità a soggetti che abbiano un potere decisionale effettivo e del tutto autonomo sulle finalità e sulle modalità dei trattamenti effettuati nel proprio ambito. Qualche dubbio sorge in relazione al secondo periodo del medesimo articolo, ma viene ugualmente smentito.

Anche se ai sensi dell'art. 6, comma 1, lett. b) del D. Lgs. 231/2001 l'Organismo di Vigilanza viene considerato come "organismo"[349], ciò non implica di per sé che possa configurarsi come titolare a prescindere da un potere decisionale effettivo rispetto alla determinazione delle finalità e dei mezzi; detto potere dev'esserci affinché il soggetto possa essere qualificato alla stregua di titolare, cosa che non si ha nel caso dell'OdV.

Il D. Lgs. 231/2001 all'art. 6 delinea i compiti dell'Organismo di Vigilanza, le cui finalità generali di prevenzione dei reati presupposto non si possono confondere con le finalità particolari dei trattamenti strumentali allo svolgimento dei medesimi compiti: una cosa è indicare i compiti di un organismo, altra cosa è definire le finalità dei molteplici trattamenti che esso deve porre in essere per svolgere tali compiti. Perciò, se può dirsi che i compiti dell'OdV sono determinati dalla legge, non può dirsi altrettanto per la tipologia dei trattamenti dei dati che esso attua e per le finalità connesse a ciascun tipo di trattamento, i quali, invece, dipendono essenzialmente dal Modello organizzativo e gestionale dell'ente vigilato[350]. Per quanto riguarda i mezzi dei trattamenti e i criteri specifici di designazione dell'OdV nulla dice la legge, vengono rimessi alla

[349] Peraltro, con una definizione "atecnica", da intendersi più propriamente come "particolare ufficio di impresa" come sostiene P. SFAMENI, *Responsabilità da reato degli enti e nuovo diritto azionario: appunti in tema di doveri degli amministratori ed Organismo di Vigilanza*, in *Rivista delle società*, Giuffrè, n.1, 2007, pp. 180 ss.

[350] cit. ASSOCIAZIONE DEI COMPONENTI DEGLI ORGANISMI DI VIGILANZA *EX* D. LGS. 231/2001, *Sulla qualificazione soggettiva dell'Organismo di Vigilanza ai fini privacy*, Milano, 2019, pp. 14 e 15.

discrezionalità dell'ente in sede di adozione dei modelli affinché l'Organismo possa essere liberamente modellato in relazione al grado di complessità aziendale di ciascuna entità.

Rimane da svolgere l'analisi critica della tesi opposta per cui l'OdV sarebbe qualificabile come responsabile del trattamento. In passato detta soluzione era sostenibile sul presupposto che si trattasse di un "responsabile interno". La figura del "responsabile interno" era ammessa fino all'entrata in vigore del GDPR e la conseguente abrogazione dell'art. 4 del D. Lgs. 196/2003 ad opera del D. Lgs. 101/2019 che hanno definitivamente fatto venir meno la concepibilità giuridica di detta figura.

Oggi, per ottenere la qualifica di responsabile bisogna essere una persona giuridica distinta dal titolare[351], caratteristica non concepibile per l'OdV, dato il suo carattere istituzionale interno rispetto all'ente vigilato[352] ovvero il suo requisito di appartenenza all'ente. Di converso, il responsabile del trattamento nasce da una decisione di esternalizzazione del titolare, il quale può decidere o di trattare i dati all'interno della propria organizzazione ovvero di delegare, in tutto o in parte, il trattamento ad un'organizzazione esterna[353].

Quindi, mancando il presupposto di una soggettività autonoma dell'OdV, necessaria affinché possa qualificarsi come responsabile ai sensi del GDPR, non risulta sostenibile nemmeno questa tesi dottrinale e l'inquadramento soggettivo dell'OdV ai fini della *privacy* risulta assorbito da quello della società vigilata della quale l'OdV è parte integrante.

In conclusione, per tutte le ragioni sopra esposte l'AODV231 ritiene che l'Organismo di Vigilanza, essendo parte dell'impresa, non possa essere qualificabile né come titolare né come responsabile del trattamento *ex* art. 4, nn. 7) e 8) del GDPR. Non è nemmeno possibile qualificare l'OdV, o i suoi membri singolarmente, come soggetti designati al trattamento *ex* art. 2-*quaterdecies* del D. Lgs. 196/2003 come novellato dal D. Lgs. 101/2018, questo sulla base del fatto che si fa esclusivamente riferimento a

[351] Così come chiarito dalla *Opinion 1/2010* del WP29.
[352] *Ex* art. 6, co.1, lett. b) del D. Lgs. 231/2001.
[353] cfr. WP29, *Opinion 1/2010*, p. 1 e 25.

persone fisiche, mentre l'OdV normalmente è un organismo collegiale ed inoltre la designazione concessa dalla norma è sottoposta all'autorità diretta del titolare senza margini di autonomia, aspetto incompatibile perché troppo restrittivo con l'istituzionale autonomia di iniziativa e controllo di cui si dota l'OdV.

Perciò, l'Associazione dei Componenti degli Organismi di Vigilanza *ex* D. Lgs. 231/2001 ritiene che, ai fini dell'osservanza delle norme relative alla protezione dei dati, l'inquadramento soggettivo dell'Organismo di Vigilanza (collegiale o monocratico) sia assorbito da quello dell'ente/società vigilata della quale, appunto, l'OdV è "parte"[354].

#### 4.7.1.2. *Il Parere del Garante per la Protezione dei Dati Personali*

L'incontro svoltosi presso la sede del Garante il 5 novembre 2019 tra l'Associazione dei Componenti degli Organismi di Vigilanza *ex* D. Lgs. 231/2001 e il Garante *privacy* ha dato vita al *Position Paper* dell'Associazione, analizzato nel paragrafo precedente e al Parere del Garante datato 12 maggio 2020, che verrà analizzato nel seguente paragrafo.

Il Garante come l'AODV231 individua le medesime fonti di trattamento dei dati personali da parte dell'OdV[355]; chiarisce che, seppur sia dotato di autonomi poteri di iniziativa e controllo per l'espletamento delle funzioni, non può essere considerato quale autonomo titolare del trattamento poiché i compiti non sono determinati dallo stesso Organismo, ma dall'Organo dirigente che ne definisce gli aspetti relativi al funzionamento, compresa l'attribuzione delle risorse, dei mezzi e delle misure di sicurezza.

Il Garante aggiunge che l'OdV non può essere considerato neppure quale responsabile del trattamento, come persona giuridicamente distinta dal titolare che agisce per conto di quest'ultimo secondo le istruzioni impartite. Il GDPR prevede una serie di

[354] cit. ASSOCIAZIONE DEI COMPONENTI DEGLI ORGANISMI DI VIGILANZA *EX* D. LGS. 231/2001, op. cit., p. 19.

[355] Per ricordare, le fonti di trattamento sono individuate nei flussi informativi, nei risultati dell'attività di controllo e nelle segnalazioni di condotte illecite o violazioni dei Modelli 231.

obblighi in capo al responsabile e la sua diretta responsabilità nel caso in cui li disattenda; diversamente, la responsabilità per gli omessi controlli sull'osservanza dei Modelli predisposti dall'azienda non ricadono sull'OdV, ma sull'ente stesso.

Il Garante definisce l'OdV nel suo complesso come parte dell'ente e l'ente stesso come titolare del trattamento che definisce le modalità di esercizio delle funzioni assegnate all'OdV e il ruolo dei singoli membri che lo compongono, quest'ultimi si atteggiano come soggetti autorizzati che dovranno attenersi alle istruzioni impartite dal titolare.

In conclusione, il Garante chiarisce che dette affermazioni si riferiscono ai flussi informativi rilevanti *ex* art. 6, commi 1 e 2 del D. Lgs. 231/2001, rimanendo escluso il ruolo che l'Organismo potrebbe acquisire in relazione alle segnalazioni in materia di *whistleblowing*. La gestione delle segnalazioni in materia di *whistleblowing* non dev'essere necessariamente attribuita all'OdV, ma è rimessa alla discrezionalità dell'ente la scelta di individuare un soggetto destinatario diverso che dovrà istruirle ed adottare i conseguenti provvedimenti. Qualora l'ente scelga di attribuire il ruolo all'OdV, secondo il Garante, questo potrebbe anche assumere la qualificazione soggettiva ai fini *privacy* di titolare e di conseguenza gli verrà attribuita la responsabilità dello specifico trattamento[356].

### 4.7.2. *DPO come membro dell'Organismo di Vigilanza, è ammissibile?*

In relazione alle figure del *Data Protection Officer* e l'Organismo di Vigilanza sorge spontanea una domanda: è ammissibile che il DPO sia un membro dell'OdV?

Prima di rispondere al quesito bisogna sempre tenere a mente una prerogativa fondamentale: l'assenza di conflitti di interessi. Detta prerogativa, in relazione al DPO è prevista all'art. 38 del GDPR; mentre, in relazione all'OdV si individua in via

[356] cfr. G. ALVERONE, *Privacy e compliance 231: il ruolo privacy degli organismi di vigilanza*, in *Diritto.it*, 2022.

interpretativa, dato che il D. Lgs. 231/2001 non fornisce indicazioni precise sulla composizione dell'OdV con l'intento di lasciare ampia discrezionalità, ma con l'unico limite del principio per cui non vi può essere identità tra controllato e controllante[357] e deve essere garantita «*l'autonomia dell'iniziativa di controllo da ogni forma di interferenza o condizionamento da parte di qualunque componente dell'ente e, in particolare, dall'organo dirigente*»[358].

Il Garante non si è ancora pronunciato in merito alla domanda prima posta e si auspica un suo celere chiarimento, in attesa si possono individuare due tesi contrapposte che animano il dibattito: da una parte vi sono coloro che sostengono la possibilità che il DPO possa essere un membro dell'OdV, dall'altra parte chi è contrario a detta eventualità.

L'orientamento prevalente è quello di mantenere distinte le due funzioni, considerando peraltro che all'interno dei reati presupposto *ex* D. Lgs. 231/2001 non vi sono quelli inerenti alla protezione dei dati personali; perciò, l'OdV non è tenuto a verificare l'applicazione o meno delle misure necessarie per il rispetto della normativa in materia di *privacy*.

Analizzando nel dettaglio le due diverse tesi, coloro che sono a favore della possibilità che il DPO possa essere membro dell'OdV si basano sulle sinergie che ravvedono nelle attività di controllo svolte da questi due soggetti. In particolare, queste sinergie si riscontrano: nei reati aventi ad oggetto il *copyright*[359] è compito dell'OdV verificare la correttezza delle licenze *software* acquistate e, tale aspetto, è anche oggetto di interesse del DPO; nelle procedure, tipiche di un Modello 231, che prevedono la gestione dei rapporti con la Pubblica Amministrazione, comprese le verifiche, da parte dei soggetti preposti, del rispetto della normativa da parte di soggetti emanazione della PA[360], tra questi vi rientra anche l'Autorità Garante; infine, nell'ambito delle procedure

[357] Cass. pen., sez. un., 24 aprile 2014, n. 38343, sent.

[358] Cass. pen., sez. V, 18 dicembre 2013, n. 4677, sent.

[359] Il *copyright* designa una riserva del diritto d'autore, che viene esplicitamente dichiarata dall'editore o dall'autore stesso, anche con la semplice apposizione del caratteristico simbolo ©, in ogni sua pubblicazione, per evitare riproduzioni non autorizzate dell'opera (cit. Enciclopedia online, in *treccani.it*).

[360] Tra i soggetti emanazione della PA, o su mandato della PA, che possono effettuare verifiche si cita, a titolo di esempio: ASL, Guardia di Finanza, INAIL.

in comune tra GDPR e Decreto 231 vi sono quelle relative alla pianificazione e gestione dell'attività di *audit* e dei controlli, per quanto riguarda i controlli svolti sia da DPO che OdV vi rientrano sicuramente quelli riferiti alle misure di sicurezza, per il DPO saranno rilevanti per tutelare i diritti e le libertà degli interessati ovvero prevenire possibili *data breach*, mentre per l'OdV avranno rilevanza per la prevenzione dei reati informatici.

Coloro che, invece, sono contrari alla possibilità che il DPO sia membro dell'OdV fanno leva, *in primis*, sul requisito dell'indipendenza richiesto al DPO, il quale, deve garantire l'assenza di conflitto di interessi, evitando qualsiasi legame che possa porre in dubbio la condizione di terzietà del controllore (DPO) rispetto all'oggetto del controllo (anche attività dell'OdV e dei membri che lo compongono)[361]. Suddetta tesi è rafforzata dal Provvedimento del Garante del 12 maggio 2020, avente ad oggetto la posizione dell'OdV, nel quale chiarisce che i membri dell'OdV sono soggetti autorizzati *ex* art. 2-*quaterdecies* del Codice *Privacy*; perciò, sottoposti al controllo del DPO in merito al rispetto delle misure tecniche ed organizzative adottate dal titolare in relazione ai trattamenti da essi svolti.

In conclusione, appoggiando la tesi prevalente, si deve ritenere inammissibile che il DPO sia un membro dell'OdV, perché l'operato dei membri dell'Organismo è oggetto di controllo da parte del DPO stesso; quindi, se il DPO rivestisse il ruolo di membro dell'Organismo vi sarebbe una sovrapposizione tra controllore e controllato, tale da creare un conflitto di interessi ed inficiare negativamente sul requisito di indipendenza.

### 4.7.3. *Flussi informativi tra DPO e OdV*

Un ulteriore aspetto che crea un collegamento tra il DPO e l'OdV riguarda i flussi informativi, i quali costituiscono uno strumento essenziale nel sistema di controllo interno perché, conoscendo e gestendo tempestivamente i rischi, permettono di prevenire la commissione di reati e la violazione del Regolamento (UE) 2016/679. Nei flussi

[361] cit. S. BONGIOVANNI, C. MOTTINO, M. PEREGO, op. cit., pp. 40 ss.

documentali periodici indirizzati all'OdV sono ricomprese le relazioni periodiche del DPO, anche rispetto alla possibilità di garantire un controllo sui reati informatici. Il *Data Protection Officer* sarà tenuto a redigere una relazione, con cadenza temporale definita, che conterrà le principali evoluzioni normative e l'eventuale aggiornamento dello strumento operativo utilizzato per organizzare i processi di *cybersecurity*.

Vige un principio di reciprocità per cui, come il DPO informa l'OdV, anche quest'ultimo dovrà informare tempestivamente il DPO, in merito a criticità riscontrate, nel corso dell'attività di vigilanza e controllo, inerenti all'applicazione della *privacy compliance*. Quindi, detti organi si confronteranno in relazione ai compiti che sono chiamati a svolgere.

Inoltre, il DPO incontra periodicamente, almeno una volta all'anno l'OdV, occasione nella quale vi sarà un ulteriore scambio di informazioni finalizzato a riferire lo stato di attuazione *privacy* che confluirà in un verbale.

Per quanto attiene alle prospettive *de iure condendo*, in caso di inserimento delle fattispecie *privacy* tra i reati presupposto, tra DPO e OdV dovrebbero aumentare le occasioni di dialogo, questo però al contempo potrebbe rafforzare le ragioni di separazione tra i due ruoli.

L'attuale scambio di informazioni reciproco favorisce l'espletamento dei rispettivi compiti del DPO e OdV, realizzando, in parte, un sistema di *compliance* integrata.

### 4.8. *Le divergenze tra i Modelli*

Le divergenze tra i Modelli di organizzazione sussistono e non si possono ignorare perché potrebbero costituire un ostacolo alla realizzazione di un Modello integrato.

Tra queste, come già analizzato nei paragrafi precedenti[362], ve ne sono alcune all'interno del processo di analisi dei rischi tali da impedire una mappatura dei rischi integrata, cioè una mappatura che tenga conto sia dei rischi connessi alle violazioni nel

[362] v.d. paragrafo 4.2.

trattamento dei dati, sia dei rischi collegati alla commissione di reati presupposto. L'analisi dei rischi avente lo scopo di individuare le aree di attività sensibili e di ridurre la commissione di illeciti, quali violazioni nel trattamento dei dati personali ovvero commissione di reati presupposto, non ha la stessa efficacia in relazione al Regolamento (UE) 2016/679 e al D. Lgs. 231/2001. La diversa efficacia sta nel fatto che la riduzione del rischio ai sensi del GDPR non implica necessariamente che le misure adottate per tale fine siano in grado di costituire esimente ai sensi del Decreto 231.

Vi sono eterogeneità anche rispetto agli Organismi di controllo, causate dai diversi obbiettivi perseguiti dall'Organismo di Vigilanza e dal *Data Protection Officer*; tali da non permettere la coincidenza di questi due ruoli in un unico soggetto comune[363]. Entrambi si atteggiano quali centri di imputazione di compiti di vigilanza, necessari affinché gli strumenti di *compliance* siano adottati ed efficacemente implementati. Difficilmente i due ruoli possono essere rivestiti da un unico soggetto, per diverse ragioni: le informazioni acquisite in relazione ad un ruolo potrebbero influenzare eccessivamente le decisioni da assumere nell'altro ruolo; gli obbiettivi perseguiti dalle normative sono differenti, il GDPR punta alla minimizzazione dei trattamenti, mentre il Decreto 231, affinché si possano dissuadere i membri dell'ente dal commettere reati, conferisce una massima estensione al controllo svolto dall'OdV; i compiti e i poteri del DPO sono determinati in maniera chiara e dettagliata, a differenza di quanto accade per l'OdV; la nomina dell'OdV è necessaria affinché il Modello 231 risulti essere adeguato, viceversa il DPO viene individuato solo in determinati casi; il requisito fondamentale di garantire un'assenza di conflitti di interesse in relazione a queste figure di vigilanza, rende impossibile l'eventualità che il DPO sia anche un membro dell'OdV.

Ulteriore differenza si ha nelle certificazioni, le quali, come visto[364], secondo la giurisprudenza non possono ritenersi esimenti ai sensi del D. Lgs. 231/2001; mentre, in relazione al GDPR sono di fondamentale importanza, si definiscono quali misure di

[363] vd. par. 4.7. e seguenti sottoparagrafi.
[364] vd. par. 4.1., p. 139.

*accountability* in grado di mitigare i rischi di perdita di riservatezza, integrità e disponibilità dei dati.

Le previsioni contenute nel GDPR si caratterizzano per una elevata specificità rispetto a come dovrà strutturarsi il Modello *privacy*; diversamente, le disposizioni del Decreto 231 stabiliscono unicamente il contenuto minimo inderogabile che dovrà avere MOGC, lasciando ampio spazio alla discrezionalità dell'ente.

Ai sensi del D. Lgs. 231/2001 l'ente risponderà solo dei reati commessi nel suo interesse o a suo vantaggio da coloro che rivestono posizioni di vertice al suo interno ovvero da chi è sottoposto alla direzione dei primi. Quindi, non si potrà addebitare la responsabilità amministrativa da reato all'ente qualora i soggetti appena menzionati commettano illeciti a danno dell'ente stesso ovvero qualora gli illeciti siano commessi nel suo interesse o vantaggio, ma da soggetti estranei all'organizzazione imprenditoriale, non sottoposti a direzione o vigilanza di coloro tramite i quali si manifesta la volontà della persona giuridica. Diversamente, il GDPR prevede l'assoggettabilità a sanzioni pecuniarie del titolare del trattamento dei dati, tutte le volte che gli si possa addebitare una violazione dei dati personali da lui processati, derivante dall'assenza o inefficacia di adeguati strumenti di *data protection*. Questo, anche qualora si concretizzi in un danno per l'ente ovvero qualora il *data breach* sia perpetrato da soggetti estranei all'ente stesso.

Infine, i Modelli 231 hanno una differente portata scriminante, se adottati ed efficacemente attuati consentono di assolvere l'ente dai reati commessi dai suoi membri. Viceversa, il GDPR non contiene una declaratoria così netta e lascia aperti spiragli di responsabilizzazione anche in capo al titolare del trattamento che abbia provveduto ad adottare una *privacy compliance* astrattamente idonea a prevenire le violazioni del Regolamento.

Le divergenze appena menzionate portano a sostenere l'impossibilità di un'integrazione tra le due normative e a preferire l'approccio tradizionale con un ragionamento a compartimenti stagni, un'esecuzione separata delle leggi e la costituzione di due differenti Modelli organizzativi, per evitare rischi e costi dovuti dalla mancata conformità alle normative.

# CONCLUSIONI

Le aziende sono tenute a conformarsi a quanto previsto dal Regolamento (UE) 2016/679, in materia di protezione dei dati personali, e quanto previsto dal D. Lgs. 231/2001, riguardo alla struttura organizzativa che dovranno adottare per evitare che gli venga attribuita una responsabilità amministrativa da reato, nel caso in cui vengano commessi, da soggetti che le compongono, degli illeciti penali. Questa legalità, per le aziende, comporta un notevole dispendio di energie, risorse e spesso diverse difficoltà da dover affrontare.

Ripercorrendo brevemente ciò che è emerso nel quarto capitolo, capitolo principe dell'elaborato che, con uno studio calato nel concreto, cerca di trovare delle soluzioni ideali per le realtà aziendali, nel confronto tra il GDPR e il D. Lgs. 231/2001, i punti di contatto emersi riguardano il MOP e il MOGC, in quanto: entrambi si basano sul criterio *Segregation of Duties*; utilizzano un *risk based approach*; prevedono un Codice etico; dispongono di organismi di controllo; stabiliscono piani di formazione per il personale aziendale; predispongono flussi informativi per agevolare le attività di controllo del DPO e dell' OdV; prevedono specifiche procedure da seguire qualora vi siano delle violazioni; possono disporre di certificazioni; infine, adottano prassi standardizzate per garantire la conformità delle attività aziendali alle normative.

Continuando con i punti di intersezione, la disciplina del *whistleblowing* richiede alle realtà aziendali di attivare sistemi per gestire le segnalazioni di illeciti commessi al loro interno e garantire una protezione adeguata contro eventuali ritorsioni al segnalante, a prescindere dalla predisposizione o meno del Modello organizzativo e non solo rispetto a segnalazioni aventi ad oggetto illeciti rientranti nel catalogo dei reati c.d. presupposto. L'azienda predispone protocolli di *whistleblowing* che implicano, inevitabilmente, un trattamento di dati personali; perciò, l'azienda stessa si qualifica alla stregua di titolare del trattamento, per cui dovrà rispettare gli obblighi e principi generali in materia di *privacy*.

Per quanto attiene alle divergenze o comunque, in generale, alle problematiche

che si possono presentare qualora si mettano a confronto il GDPR e il Decreto 231, in breve si è visto che: nonostante entrambi i sistemi di *compliance* richiedano un'analisi dei rischi questa potrebbe non essere equivalente; si dovrà verificare, caso per caso, se l'analisi del rischio attuata dall'azienda riesca, contemporaneamente, a scongiurare le violazioni nel trattamento dei dati personali ed avere efficacia esimente per l'ente nel caso di commissione di reati presupposto dai soggetti che lo compongono. Ulteriore differenza, in senso stretto, attiene alle condotte sanzionate dalle normative, il Decreto 231 sanziona i reati commessi da un soggetto facente parte dell'organico dell'ente, nell'interesse o vantaggio dell'ente stesso; mentre, il GDPR sanziona il titolare del trattamento ogniqualvolta gli si addebiti una violazione della protezione dei dati personali da lui trattati, per un'inefficacia o inesistenza di adeguati strumenti di protezione, anche qualora detta violazione sia commessa da un soggetto esterno all'impresa ovvero sia commessa nell'interesse e/o vantaggio dell'impresa stessa.

I Modelli di organizzazione hanno una differente portata scriminante, i MOGC se adottati ed attuati efficacemente escludono la responsabilità dell'ente, mentre i MOP, anche se astrattamente idonei a prevenire violazioni, potrebbero comunque attribuire una responsabilità all'ente.

Continuando con le problematiche che potrebbero ostacolare l'integrazione queste si individuano nel principio di *accountability*; principio base per il GDPR, ma applicabile anche nel Decreto 231, in quanto entrambe le normative puntano ad una maggiore responsabilizzazione dell'ente. Detto principio entra in conflitto con il privilegio contro l'autoincriminazione; per cui l'ente, qualora venga commesso un illecito, dal quale potrebbe conseguirne una sua responsabilità penale, non dovrebbe essere obbligato a dare un contributo conoscitivo che potrebbe comportare la sua incriminazione. Il GDPR richiede una collaborazione attiva dell'ente in queste situazioni senza garantire il *nemo tenetur se detegere*, garanzia che vanta l'accusato in un processo penale. Questo principio si dovrebbe applicare in un processo penale in senso stretto, ma a seguito di una serie di pronunce della Corte EDU, si dovrebbe estendere anche alla fase prodromica, amministrativa e dedicata alla collaborazione; sulla base del fatto che le sanzioni

applicate, nel caso in cui l'ente risulti inadempiente, sono qualificate solo formalmente come amministrative perché nella sostanza si devono considerare come penali.

Entrambe le normative prevedono degli organi di sorveglianza, il *Data Protection Officer* e l'Organismo di Vigilanza, pur svolgendo entrambi un'attività di controllo sulla conformità normativa dell'organizzazione aziendale, non sono pienamente sovrapponibili. Vi sono delle differenze, in particolare, relativamente ai diversi obbiettivi perseguiti, tali da non permettere una loro integrazione; bisogna comunque riconoscere che le loro funzioni, per essere efficacemente espletate, implicano una reciproca collaborazione.

Alcune criticità potrebbero sorgere in un prossimo futuro, è il caso del problema del *ne bis in idem* sostanziale. Qualora le fattispecie di illeciti in materia di *privacy* venissero inserite all'interno del catalogo dei reati presupposti, si dovrà porre il problema del doppio binario sanzionatorio; ad uno stesso fatto si applicherà sia una sanzione penale che una sanzione solo formalmente amministrativa perché nella sostanza è anch'essa penale.

Posto che molteplici possono essere i sistemi di *compliance* da adottare, analizzati nel dettaglio il GDPR, il D. Lgs. 231/2001 e una volta riconosciuti i loro punti di contatto e le loro divergenze, si può giungere alla conclusione per cui pare utile ricorrere ad una soluzione che abbracci le diverse discipline, attraverso l'utilizzo dei medesimi metodi di analisi del rischio, dei medesimi criteri per il controllo e per la prevenzione dello stesso, pur mantenendo le specifiche peculiarità. Questa è la *compliance* integrata: un unico insieme di flussi informativi, documenti, protocolli che disciplinino, con una metodologia comune, le varie aree di rischio dell'ente. I sistemi organizzativi, a protezione della società stessa e dei dati da essa trattati, possono essere intesi come complementari viste le varie e rilevanti analogie. Le normative si prestano a letture simmetriche stante la comune *ratio legis*: garantire sicurezza e prevenzione. In conclusione, un progetto organizzativo integrato è un'opportunità innovativa per la legalità di impresa che permette, non solo di ridurre i costi, ma anche di evitare inutili duplicazioni, favorendo l'uniformità delle *policy* aziendali e potenziando le sinergie tra i processi aziendali.

## BIBLIOGRAFIA


E. AMATI, *La responsabilità da reato degli enti,* UTET Giuridica, 2007.

G. ALVERONE, *Privacy e compliance 231: il ruolo privacy degli organismi di vigilanza*, in *Diritto.it*, 2022.

E. AMBROSETTI (et al.), *Diritto penale dell'Impresa*, V Edizione, Bologna, Zanichelli Editore, 2022.

ASSOCIAZIONE DEI COMPONENTI DEGLI ORGANISMI DI VIGILANZA EX D. LGS. 231/2001, *Sulla qualificazione soggettiva dell'Organismo di Vigilanza ai fini privacy*, Milano, 2019.

ASSOCIAZIONE BANCARIA ITALIANA, *Linee guida dell'Associazione Bancaria Italiana per l'adozione di modelli organizzativi sulla responsabilità amministrativa delle banche*, 2004.

P. BALBONI, F. TUGNOLI, *Reati informatici e tutela dei dati personali: profili di responsabilità degli enti*, in *Giurisprudenza penale web*, 1-*bis*, 2021.

E. BARRACO, A. SITZIA, *GDPR in 10 punti*, IPSOA, Milano, 2018.

F. BIANCHI, *La funzione compliance e il Modello 231*, in *Rivista 231*, 2010.

A. BIASIOTTI, *Il nuovo regolamento europeo sulla protezione dei dati*, III ed., Roma, 2018.

L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo*, Milano, 2016.

S. BONGIOVANNI, C. MOTTINO, M. PEREGO, *Formulario del DPO Norme, giurisprudenza, strumenti operativi e modelli di atti,* G. Giappichelli, 2021.

A. CADOPPI [et. al.], *Cybercrime*, I ed., UTET Giuridica, Milano, 2019.

L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale Scientifica, Napoli, 2017.

P. CALVI, *DPO la presa in carico di un'azienda: le fasi di assessment*, in *cybersecurity360.it*, 2021.

F. CARRARA, *Momento consumativo del furto*, in *Lineamenti di pratica legislativa penale*, Torino, 1874.

M. CASELLATO, A. DI MAIO, D. LA MUSCATELLA, *Il nodo gordiano dello "sviamento di potere" nell'accesso abusivo ad un sistema informatico, tra suggestioni dogmatiche e riflessioni giurisprudenziali*, in *Cassazione penale*, fasc. n. 7, 2019.

M. CIRIGLIANO, *Dal D. Lgs. 231/2001 al GDPR (Regolamento UE 2016/679) attraverso il D. Lgs. 81/2008: il modello di organizzazione gestione e controllo integrato, avanguardia di un progetto di attuazione normativa combinata, un'opportunità per le aziende da intuire e cogliere*, in *Giurisprudenza penale web*, 1-*bis*, 2021.

CONFINDUSTRIA, *Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo, ai sensi del decreto legislativo 8 giugno 2001, n. 231*, 2021.

CONSIGLIO NAZIONALE FORENSE, *FAQ per gli Ordini degli Avvocati in materia di protezione dei dati personali*, pubblicate il 28 marzo 2018.

G. CORASANITI, R. PRODI, L. LOEVINGER, *Esperienza giuridica e sicurezza informatica*, Giuffrè, Milano, 2003.

CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, comunicato stampa n. 70/14 Lussemburgo, in *curia.europa.eu*, 13 maggio 2014.

COUNSEIL DE L'EUROPE, *Recommandation n. R (89) 9*, Strasbourg, passim, 1990.

D. COSTA, *I modelli 231 e la compliance aziendale sulla tutela dei dati personali. Aspetti comuni e divergenze a quattro anni di distanza dall'entrata in vigore del GDPR*, in *Giurisprudenza penale web*, 2020.

EUROPEAN DATA PROTECTION BOARD, *Guidelines 4/2019 on Article 25*, *Data Protection by Design and by Default,* Version 2.0, Adopted on 20 October 2020.

A. FABERI, *Privilegio contro l'autoincriminazione e accountability. Alcuni profili problematici*, in *Archivio penale*, n. 2, 2021.

G. FIANDACA, E. MUSCO, *Diritto penale, parte generale.*, VIII ed., Zanichelli, Bologna, 2023.

E. FILADELFIO, *Least privilege: dati al sicuro da accessi non autorizzati col principio del privilegio minimo*, in *cybersecurity360.it*, 2021.

G. FINOCCHIARO, *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017.

D. FIORONI, *Attacco Hacker a Leonardo Spa, 2 arresti*, in *poliziadistato.it*, 5 dicembre 2020.

R. FLOR, *Dalla data retention al diritto all'oblio*, 2014.

P. FRANCESCHETTI, *Pena*, in *AltalexPedia*, 2017.

L. FRUSCIONE, A. GIUSTINI, *Gli aspetti organizzativi dell'attività di controllo del Modello 231*, in *Rivista 231*, 2019.

M. FUMO, *La condotta nei reati informatici,* in *Archivio Penale*, fascicolo 3, 2013.

P. GALDIERI, *Il Diritto penale dell'informatica: legge, giudice e società*, G. Giappichelli Editore, Torino, 2021.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Amministratori di sistema: occorre massima trasparenza sul loro operato. Il Garante fissa i criteri, quattro mesi per mettersi in regola*, in *garanteprivacy.it*., 2008.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Faq sul Resposabile per la Protezione dei Dati (RPD) in ambito privato*, doc. web n. 8036793, in *garanteprivacy.it*, 26 marzo 2018.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, parere n. 304, *Schema di Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali – procedure per la presentazione e gestione delle segnalazioni esterne*, in *garanteprivacy.it*, 6 luglio 2023.

A. GARGANI, *Imputazione del reato agli enti collettivi e responsabilità penale dell'intraneo: due piani irrelati?*, in *Diritto penale e processo*, volume 8, 2002.

M. IASELLI, *Web Service Provider, guida all'ISP: cos'è, regime e tipologie di responsabilità*, in *Altalex*, 2019.

H. JESCHECK, T. WEIGEND, *Lehrbuch des Strafrechts - Allgemeiner Teil*, V ed., Berlino, 1996.

P. LA SELVA, *La responsabilità amministrativa degli enti*, in *iusinitinere.it*, 2017.

S. LONGHI, *La persona giuridica come soggetto di responsabilità penale*, in *Rivista penale*, Torino, 1906.

L. LUPARIA [et. al.], A. MONTI (a cura di), *Cybercrime e responsabilità da reato degli enti: prevenzione, modello organizzativo e indagini preliminari*, Giuffrè, Milano, 2022.

F. MANTOVANI, *Diritto penale - Parte generale*, X ed., Padova, 2020.

G. MARINO, *Il profitto del reato alla luce della teoria generale del reato e la sua rilevanza in tema di confisca. Il profitto, il prodotto ed il prezzo del reato: analisi dogmatica*, in *Altalex*, 2023.

P. MAROCCO, Vocabolario Treccani online, in *treccani.it,* 2015.

F. MARTINELLI*, Il fenomeno del whistleblowing,* in *Giurisprudenza penale web*, 2017.

M. MARTORANA, A. TESORO, A. BARBERISI (a cura di), *Gdpr: guida pratica agli adempimenti privacy,* CEDAM, 2018.

P. MILITE, *Documento e documentazione*, in *Riv. Giuridica Italiana*, 2000.

T. J. MIRÒ D'ANIELLO, *L'art. 40 cpv c.p. e la sua compatibilità con alcune figure criminose*, in *iusinitinere.it*, 2019.

E. MUSCO, *Le imprese a scuola di responsabilità tra pene pecuniarie e misure interdittive,* in *Diritto e giustizia*, n. 23, 2001.

E. NARDELLI, *La rivoluzione informatica: conoscenza, consapevolezza e potere nella società digitale*, Edizioni Themis, 2022.

N. NOSENGO, Treccani online, in *treccani.it*, 2006.

OCSE, *Computer-related Crime: Analysis of Legal Policy*, Parigi, 1986.

F. PALAZZO, *Corso di diritto penale, parte generale*, Torino, 2016.

C. E. PALIERO, *Il d.lgs. 8 giugno 2001 n. 231: da ora in poi, societas delinquere (et puniri) potest*, in *Corriere giuridico*, 2001.

M. PEREGO, C. PONTI, *La protezione dei dati personali ed il Modello Organizzativo D. Lgs. 231/2001*.

M. PRENSKY, "*Digital Natives, Digital Immigrants",* on the *Horizon MCB University Press*, Vol. 9 No. 5, October 2001.

L. PICOTTI (et. al.)*, Il diritto penale dell'informatica all'epoca di web,* CEDAM, Padova, 2004.

L. PICOTTI*, Il dolo specifico*. *Un'indagine sugli "elementi finalistici" delle fattispecie penali*, Milano, 1993.

L. PICOTTI, *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in *riv. Trim. dir. Pen. ec*., 2011.

C. PIERGALLINI, *Sistema sanzionatorio e reati previsti dal codice penale*, Ipsoa, Milano, 2001.

N. PISANI, *I requisiti di autonomia ed indipendenza dell'organismo di vigilanza istituito ai sensi del d. lgs. 231/2001*, in *La responsabilità amministrativa delle società e degli enti*, 2015.

C. PIVATO, *DPO e organismo di vigilanza (ODV): definire ruoli e competenze per evitare conflitti di interesse*, in *cybersecurity360.it*, 2019.

C. E. PONTI, S. PERSI, M. PEREGO, *Il modello organizzativo privacy - MOP*, Giuffrè, 2020.

S. RODOTÀ, *Intervista su Privacy e libertà,* Editori Laterza, 2005.

M. ROMANO, *La responsabilità amministrativa degli enti, società o associazioni: profili generali,* in *Governo dell'impresa e mercato delle regole, Scritti giuridici per Guido Rossi*, vol. II, Milano, 2002.

P. SALVEMINI, *Il doppio binario sanzionatorio al vaglio della Corte di Giustizia: la Grande Sezione si pronuncia sulle questioni pregiudiziali*, in *diritticomparati.it*, 2018.

C. SANTORIELLO, *Attività dell'organismo di vigilanza e obbligo di segretezza in capo ai suoi componenti*, in *La responsabilità amministrativa delle società e degli enti*, 2015.

M. H. SCHETTINO, *Compliance 231 e whistleblowing: ecco le novità*, in *Il Sole 24 Ore*, 2023.

P. SFAMENI, *Responsabilità da reato degli enti e nuovo diritto azionario: appunti in tema di doveri degli amministratori ed Organismo di Vigilanza*, in *Rivista delle società*, n.1, Giuffrè, 2007.

B. SCHNEIER, J. KELSEY, *Cryptographic support for secure logs on un-trusted machines*, in *The 7th USENIX Security Symposium Proceedings*, USENIX Press, January 1998.

G. SIRILLI, *Enciclopedia della Scienza e della Tecnica*, Voll. I-VI Lessico, Istituto dell'Enciclopedia Italiana, Roma, 2008.

G. URICCHIO, *Modello Privacy e Modello Organizzativo. Approcci e similitudini tra la disciplina relativa al trattamento dei dati personali ai sensi del Regolamento UE 2016/679 e la disciplina del D. Lgs. 231/2001*, in *Altalex*, 2021.

G. VACIAGO, *Compliance 231. Modelli organizzativi e OdV tra prassi applicative ed esperienze di settore*, Gruppo Sole 24 Ore, Milano, 2020.

S.D. WARREN, L.D. BRANDEIS, *The Right to Privacy*, in *Harvard L. Rev.*, 1890.

WORKING PARTY ART. 29, *Opinion 1/2010 on the concepts of "controller" and "processor"*, 2010.

WORKING PARTY ART. 29, *Guidelines on Data Protection Officers ("DPOs")*, WP243rev.01, 2016.

WORKING PARTY ART. 29, *Guidelines on Data Protection Impact Assessment ("DPIA") and determining whether processing is "likely to result on a hight risk" for the purposes of Regulation 2016/679*, WP248rev.01, 2017.

M. ZIZI, Treccani online, in *treccani.it*, 2006.

S. ZUBOFF, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Profile Books Ltd, 2018.

## SITOGRAFIA


www.altalex.it

www.brocardi.it

www.cnil.fr

www.coe.int

www.cortedicassazione.it

www.cybersecurity360.it

www.curia.europa.eu

www.data.europa.eu

www.dejure.it

www.diritto.it

www.diritticomparati.it

www.dlapiper.com

www.ec.europa.eu

www.edpb.europa.eu

www.enisa.europa.eu

www.eur-l*ex*.europa.eu

www.europarl.europa.eu

www.filodiritto.com

www.garanteprivacy.it

www.giurisprudenzapenale.com

www.hoepli.it

www.iusinitinere.it

www.jstor.org

www.microsoft.com

www.osservatorio-231.it

www.politicheeuropee.gov.it

www.poliziadistato.it

www.privacy.it

www.protezionedatipersonali.it

www.riskmanagement360.it

www.rivistagiuridica.it

www.servizi.gpgp.it

www.smartius.it

www.treccani.it

www.wikipedia.it

www.wolterskluwer.com

## GIURISPRUDENZA

CEDU, 8 giugno 1976, *Engel e altri* c. *Paesi Bassi*.

CEDU, 21 febbraio 1984, *Öztürk* c. *Germania*.

CEDU, 24 febbraio 1994, *Bendenoun* c. *Francia*.

CEDU 23 novembre 2006, *Jussila* c. *Finlandia*.

CEDU, 4 marzo 2013, *Grande Stevens* c. *Italia*.

CEDU, 10 febbraio 2015, C-53753/12, *Kiiveri* c. *Finlandia*.

CEDU, 15 novembre 2016, *A. e B.* c. *Norvegia*.

Corte Giust. UE 13 maggio 2014, causa C-131/12, *Google Spain SL, Google Inc.* c. *Agencia Española de Protecciòn de Datos (AEPD), Mario Costeja Gonzàlez.*

Corte Giust. UE, Grande sezione, 20 marzo 2018, causa C-537/16, *Garlsson Real Estate SA e altri.*

C. Cost., 30 dicembre 1998, n. 456.

C. Cost., 30 aprile 2021, n. 84.

Cass. civ., sez. III, 27 maggio 1975, n. 2129, sent.

Cass. civ., sez. VI, 9 luglio e 28 settembre 2020, n. 20358, ord.

Cass. pen., sez. II, 30 gennaio 2006, n. 3615, sent.

Cass. pen., sez. VI, 25 gennaio 2013, n. 21192, sent.

Cass. pen., sez III, del 16 luglio 2013, n. 7504, sent.

Cass. pen., sez. V, 18 dicembre 2013, n. 4677, sent.

Cass. pen., sez VI, 24 gennaio 2014, n. 3635, sent.

Cass. pen., sez. V, 30 gennaio 2014, n. 4677, sent.

Cass. pen., sez. un., 24 aprile 2014, n. 38343, sent.

Cass. pen., sez. un., 18 settembre 2014, n. 38343, sent.

Cass. pen., sez. III, 5 febbraio 2015, n. 40103, sent.

Cass. pen., sez. II, 27 settembre 2016, n. 52316, sent.

Cass. pen., sez. II, 9 dicembre 2016, n. 52316, sent.

Cass pen., sez. un., 22 giugno 2017, n. 41588, sent.

Cass. pen, sez. VI, 13 settembre 2017, n. 41768, sent.

Cass., Relazione n. III/01/2013, Roma, 22 agosto 2013.

C. Ass. App., Torino, 28 febbraio 2013, n. 31095, sent.

Seconda C. di Ass., Torino, 14 novembre 2011, n. 31095, sent.

G.i.p. Trib. Roma,4 aprile 2003, ord.

G.i.p. Trib. Milano, 20 settembre 2004, n. 30.382-03, ord.

G.i.p. Trib. Milano, 09 novembre 2004, *Esame dell'idoneità dei modelli di organizzazione, gestione e controllo ex artt 6 e 7 d.lg. 231/2001,* ord.

G.i.p. Trib. Napoli, 26 giugno 2007, *Idoneità del Modello di organizzazione e gestione per la prevenzione dei reati presupposto*, ord.