ANDREA ROBERTO MUSOLINO

# PRIVACY E RESPONSABILITÀ SOCIALE D'IMPRESA:

## LA CERTIFICAZIONE ISO/IEC 27701:2019 E L'IMPLEMENTAZIONE DEL PRIVACY INFORMATION MANAGEMENT SYSTEM

DOTTORATO DI RICERCA IN
COMUNICAZIONE, RICERCA SOCIALE E MARKETING

**Facoltà di Scienze Politiche, Sociologia, Comunicazione**

**Dipartimento di Comunicazione e Ricerca Sociale**

**DOTTORATO DI RICERCA IN**

**COMUNICAZIONE, RICERCA SOCIALE E MARKETING**

CURRICULUM IN MARKETING - XXXIV CICLO

SECS-P/08 – ECONOMIA E GESTIONE DELLE IMPRESE

# PRIVACY E RESPONSABILITÀ SOCIALE D'IMPRESA:

# LA CERTIFICAZIONE ISO/IEC 27701:2019 E L'IMPLEMENTAZIONE DEL PRIVACY INFORMATION MANAGEMENT SYSTEM

**Candidato**: DR. ANDREA ROBERTO MUSOLINO

**Supervisor**: RAFFAELLA MESSINETTI
PROFESSORE ORDINARIO DI ISTITUZIONI DI DIRITTO PRIVATO
DIPARTIMENTO DI SCIENZE POLITICHE

**Tutor**: CARMELO LOMBARDO
PROFESSORE ORDINARIO DI SOCIOLOGIA GENERALE
DIPARTIMENTO DI COMUNICAZIONE E RICERCA SOCIALE

# INDICE DEI CONTENUTI

# PREMESSA

# IL RITORNO DEGLI INVESTIMENTI PRIVACY

Quando a metà degli anni Novanta fece capolino la prima legislazione in materia di *privacy* sull'onda della «Direttiva madre europea» (95/46/CE), la disciplina era talmente innovativa che ci si soffermava a disquisire sulla dizione corretta (inglese o americana) con cui pronunciare il termine. Nel corso degli ultimi vent'anni la *privacy* è divenuta una questione di sostanza, anziché di forma: lo stanno a dimostrare, a titolo meramente esemplificativo ma non esaustivo, (a) i recenti scandali internazionali, come il caso *Cambridge Analytica*[1], i nuovi (b) fenomeni lesivi della riservatezza (es. *neuroprivacy*) e (c) problemi di tutela del diritto alla protezione dati (es. profilazioni e decisioni totalmente o parzialmente automatizzate). La questione della tutela della riservatezza è riuscita via via a farsi strada nei comportamenti collettivi grazie ai richiami all'attenzione sull'uso dei dati personali che le regole di oltre vent'anni fa hanno introdotto. L'avvento del Regolamento Europeo 2016/679 ha segnato ufficialmente l'inizio dell'era del *General Data Protection Regulation*

[1] Lo scandalo dei dati *Facebook-Cambridge Analytica* è stato uno dei maggiori scandali politici avvenuti all'inizio del 2018, quando fu rivelato che *Cambridge Analytica* aveva raccolto i dati personali di 87 milioni di *account Facebook* senza il loro consenso e li aveva usati per scopi di propaganda politica. È stato definito come un momento di spartiacque nella comprensione pubblica del valore dei dati personali e di conseguenza, provocando un forte calo del prezzo delle azioni di *Facebook*, si è chiesto una regolamentazione più rigorosa sull'uso dei dati personali da parte delle aziende tecnologiche.

(GDPR) e la fine dell'era pionieristica della protezione dei dati personali mediante l'abrogazione della «Direttiva madre» n. 95/46/CE, figlia di un dibattito culturale e giuridico sul trattamento dei dati ormai datato. L'incessante evoluzione tecnologica e il conseguente mutamento di scenario hanno imposto per la prima volta la definizione di un quadro normativo comune vincolante per tutti gli Stati membri dell'Unione Europea, con l'obiettivo di uniformare e armonizzare la disciplina, eliminando le barriere che le frammentazioni normative hanno creato nel corso del tempo. Il Regolamento UE 2016/679 si fonda sull'idea che le attività di trattamento dei dati debbano essere rivolte al servizio dell'uomo in un'ottica di tutela globale e complessiva. Da questo assunto discende che il diritto alla protezione dei dati non è un diritto assoluto, ma un diritto che viene riconosciuto per la sua funzione sociale e che va, pertanto, contemperato di volta in volta con gli altri diritti fondamentali dell'uomo rilevanti e prevalenti, come, ad esempio, il diritto alla libertà di espressione o il diritto al rispetto della vita privata e familiare. Le sempre maggiori istanze per la protezione dei dati e la definitiva efficacia in tutta l'Unione Europea del GDPR, con la piena vigenza anche delle sanzioni previste per le violazioni, hanno portato ad un importante passo in avanti nella definizione di schemi di certificazione dei trattamenti. Il GDPR stabilisce a carico del titolare e del responsabile del trattamento il c.d. principio di responsabilizzazione (o *accountability*). Questo si traduce nell'adozione di misure tecniche ed organizzative adeguate volte a garantire e dimostrare che il trattamento dei dati personali posto in essere è conforme ai principi stabiliti dal Regolamento UE 2016/679. Con il principio di *accountability* il legislatore europeo ha voluto garantire il massimo rispetto delle regole di correttezza e trasparenza nell'utilizzo dei dati personali, imponendo al titolare e al responsabile un comportamento

proattivo e concreto, volto a prevenire i rischi cui potrebbero essere sottoposti i dati personali trattati. Il principio di responsabilizzazione è emerso come tema critico nella legislazione, nelle politiche e nelle prassi globali sulla *privacy*. Le organizzazioni devono essere responsabili dell'attuazione dei requisiti applicabili in materia di protezione dei dati e devono farlo per essere in grado di dimostrare la loro conformità. Una maggiore responsabilità si traduce in maggiori benefici: le aziende con valutazioni di responsabilità più elevate sperimentano minori danni economici legati alle violazioni e maggiori ritorni. Le certificazioni per la *privacy* stanno influenzando sempre più le decisioni di acquisto nella scelta di un *vendor*. In particolare, ISO/IEC 27701:2019 è stata progettata per essere applicata sia dai titolari che dai responsabili del trattamento ed è fondata su un approccio basato sul rischio, in modo che ogni operatore che voglia essere conforme affronti i rischi specifici riguardanti il trattamento dei dati. La norma è quindi applicabile per tutte le organizzazioni, qualsiasi sia la loro dimensione e il loro settore di attività ma, al contempo, ancora è di difficile attuazione per i professionisti e le piccole e medie imprese (PMI), anche se è verosimile che queste ultime debbano a breve tenerne conto per un migliore adeguamento al GDPR e agli *standard* di sicurezza. Poiché i mercati continuano a evolvere, le imprese dovrebbero considerare seriamente la possibilità di continuare ad investire e dare priorità agli investimenti in ambito *privacy* al fine di ottenere certificazioni esterne e maggiore trasparenza nelle attività di elaborazione. La protezione dei dati rappresenta una nuova ed efficace forma di Responsabilità Sociale d'Impresa (RSI) che deve essere sempre più concepita dalle organizzazioni come risorsa e non come un costo o un mero adempimento burocratico. È sempre più necessario andare oltre il minimo indispensabile richiesto

dalle leggi in quanto la *privacy* è un imperativo di *business* e le imprese stanno constatando ritorni molto positivi sui loro investimenti[2]. Per questo motivo occorre creare una forte *governance* organizzativa e *accountability* per poter dimostrare agli *stakeholder* interni ed esterni la maturità del programma e l'impegno in materia di *privacy*. Tale architettura giuridica dei meccanismi di responsabilità prevede due livelli, dei quali il primo è costituito da un obbligo di base vincolante per tutti i titolari del trattamento, consistente nell'attuazione di misure e procedure e nella conservazione delle relative prove, mentre il secondo livello include sistemi di responsabilità di natura volontaria eccedenti le norme di legge minima, in relazione ai principi fondamentali di protezione dei dati (tali da fornire garanzie più elevate di quelle prescritte dalla normativa vigente) e/o

[2] CISCO SYSTEMS INC. (2020), *Data Privacy Benchmark Study*. Lo studio, effettuato con la procedura doppio-cieco, ha raccolto i dati provenienti da interviste condotte su oltre 2800 aziende in 13 Paesi (inclusa l'Italia) e mostra per la prima volta un ritorno sugli investimenti (ROI) effettuati nell'ambito della riservatezza dei dati. Le aziende ottengono benefici pari a 2,7 volte (2,4 per l'Italia) il loro investimento iniziale e oltre il 40% ottiene benefici pari ad almeno il doppio della spesa sostenuta in materia di *privacy*. Rispetto al 40% del 2019, oltre il 70% degli intervistati dichiara di ottenere significativi vantaggi di *business* grazie alle iniziative messe in campo per la tutela della *privacy* che vanno oltre la conformità, tra cui una migliore agilità, un maggiore vantaggio competitivo, una maggiore attrattiva per gli investitori e una maggiore fiducia da parte dei clienti. Le aziende con valutazioni di responsabilità più elevate tengono in maggiore considerazione la protezione dei propri dati, sperimentano minori danni economici legati alle violazioni, minori ritardi nelle vendite e maggiori ritorni finanziari. Secondo le evidenze emerse dallo studio, l'82% delle aziende (89% in Italia) vede le certificazioni per la *privacy* (es. *ISO 27701*, *EU/Swiss-US Privacy Shield* e *APEC Cross Border Privacy Rules system*) come fattore chiave alla base delle decisioni d'acquisto nella scelta di un *vendor*. India e Brasile sono in cima alla lista con il 95% degli intervistati che concorda con questa visione. Per maggiori approfondimenti: https://www.cisco.com/.

intermedi modalità di attuazione di garanzia dell'efficacia delle misure (norme di attuazione) e consistente nell'obbligo di conformarsi. Un'impresa che adotti un comportamento socialmente responsabile, valutando e rispondendo alle aspettative economiche, ambientali e sociali di tutti gli *stakeholders* travalicando il minimo impregno previsto dalla legge, coglie l'obiettivo di creare valore e conseguire un vantaggio competitivo. Al contrario, comportamenti poco etici o la mancanza di strategie di sostenibilità e responsabilità sociale delle imprese possono danneggiare la reputazione di un'azienda e renderla meno attraente per gli azionisti, con conseguente riduzione dei profitti. In altri termini, qualora le imprese decidessero spontaneamente di aderire alla RSI, non si limiteranno a soddisfare gli obblighi giuridici, ma potranno andare oltre investendo ulteriormente nel capitale umano e nei rapporti con gli innumerevoli *stakeholders*. La inevitabile conseguenza è il mutamento del ruolo e della concezione dell'impresa stessa: si assiste al passaggio dalla logica del profitto e dello sviluppo a discapito della società civile alla visione eticamente orientata dell'attività di impresa. Le imprese, in quanto organi dello Stato-comunità, avrebbero il compito di promuovere lo sviluppo ed il benessere della comunità stessa attraverso la soddisfazione degli interessi del consumatore e del lavoratore, pena l'assunzione di responsabilità etica nei confronti della stessa collettività. La presente monografia è il risultato di anni di studi condotti sul tema e non intende certamente prendersi meriti di esaustività. Dichiaro di non aver alcun conflitto di interessi e auguro buona lettura a quanti si accingono a sfogliare le pagine del presente elaborato di tesi dottorale.

*Andrea Roberto Musolino*

# SEZIONE PRIMA

## PRIVACY E RESPONSABILITÀ SOCIALE D'IMPRESA:

## APPROCCIO DOTTRINALE

## E THEORETICAL BACKGROUND

# CAPITOLO 1

# L'IMPRESA SOCIALMENTE RESPONSABILE

**SOMMARIO:** 1. Introduzione – 2. L'inquadramento normativo europeo e italiano di riferimento e ambito di applicazione – 3. Evoluzione storica del concetto di responsabilità sociale d'impresa nella letteratura manageriale – 4. Marketing socialmente responsabile: strategia d'impresa e misurazione della performance – 5. Funzione sociale ed etica nel governo d'impresa.

## 1. Introduzione

La gestione responsabile è un imperativo su cui fondare la gestione d'impresa che impone di rivedere le proprie pratiche e i rapporti con gli innumerevoli *stakeholder*. L'insieme delle preoccupazioni e impegni di natura etica e filantropica nella visione strategica d'impresa viene identificato nella letteratura manageriale con il nome di Responsabilità Sociale d'Impresa (RSI) o, in inglese, *Corporate Social Responsibility* (CSR). Non vi è unanimità nel definire cosa si intende esattamente con RSI né tantomeno sulla locuzione da adottare: in questo contesto, sono proposti anche termini alternativi con significato affine, come «cittadinanza d'impresa», «sostenibilità d'impresa» e «*corporate accountability*». Si tratta di un concetto sul quale le imprese sono sempre più chiamate a riporre la loro attenzione e a sviluppare una propria politica in merito. Presupposto di fondo della RSI è il principio di *accountability* (responsabilizzazione), ovvero il dovere di rendicontare in modo completo e trasparente il proprio

impegno sociale ai pubblici di riferimento. A questa necessità le imprese rispondono con innumerevoli attività di rendicontazione e in quest'ottica diventa fondamentale la misurazione delle *performance* anche in ambiti diversi da quella tipicamente economico-finanziaria. Da un lato, l'attività di monitoraggio permettere all'impresa di effettuare un'analisi costi-benefici e valutare l'effettiva convenienza economica degli obiettivi sociali perseguiti e dall'altro garantisce una comunicazione affidabile ed esaustiva in grado di soddisfare le aspettative degli *stakeholder*.

## 2. L'inquadramento normativo europeo e italiano di riferimento e ambito di applicazione

Nel 2001 l'Unione Europea pubblica il Libro Verde[3] *Promuovere un quadro europeo per la responsabilità sociale delle imprese* e lancia una vasta campagna di sensibilizzazione mirata a promuovere l'integrazione volontaria della responsabilità sociale nella gestione strategica delle imprese. La prima definizione indicata

[3] LIBRO VERDE (anche detto *Green Paper*) - *Promuovere un quadro europeo per la responsabilità sociale delle imprese* presentato dalla Commissione delle Comunità Europee. Bruxelles, 18 luglio 2001. COM (2001) 366 definitivo. I fattori individuati dal c.d. Libro Verde sono: 1) le nuove preoccupazioni e attese dei cittadini, dei consumatori, delle pubbliche autorità e degli investitori in termini di attenzione alla sostenibilità e allo sviluppo; 2) i criteri di tipo etico e socio-ambientale che influiscono sempre di più sulle scelte di individui e istituzioni; 3) le pressioni delle ONG (Organizzazioni Non Governative), dalle mobilitazioni civili alle campagne di boicottaggio; 4) le crescenti inquietudini suscitate dal deterioramento dell'ambiente provocato dall'attività economica; 5) la trasparenza garantita dai mezzi di comunicazione e dalle moderne tecnologie dell'informazione e della comunicazione nell'attività delle imprese.

dall'Unione Europea designa la responsabilità sociale come il concetto secondo il quale le imprese inseriscono su base volontaria le preoccupazioni sociali ed ambientali nelle loro operazioni commerciali e nei loro rapporti con le parti interessate. La definizione implica dunque che essere socialmente responsabili significa andare oltre il semplice rispetto della normativa vigente investendo maggiormente nel capitale umano, nell'ambiente e nelle relazioni con gli *stakeholder* per aumentare la propria competitività[4]. Nel 2010 la Commissione Europea presenta la *Strategia Europa 2020*, elaborata con l'obiettivo di agevolare l'uscita dalla crisi economica e delineare un modello di sviluppo per rispondere in maniera adeguata alle sfide del decennio 2010-2020[5]. La strategia decennale sostiene la responsabilità sociale come elemento fondamentale per garantire la fiducia a lungo termine dei lavoratori e dei consumatori e si pone cinque ambiziosi obiettivi in materia di occupazione, innovazione, clima/energia, istruzione e

[4] CERANA N. (a cura di) (2004), *Comunicare la responsabilità sociale. Teorie, modelli, strumenti e casi d'eccellenza*, FrancoAngeli, Milano. L'autrice, a pag. 27 op. cit., sostiene che "la responsabilità sociale sta dunque diventando un tema di stretta attualità ma anche […] una sfida per le imprese in quanto far proprio volontariamente questo approccio significa incidere in profondità sull'insieme dei modelli di gestione dell'impresa [e quindi] adottare un nuovo paradigma di *corporate governance* in cui diventano centrali il rapporto con gli *stakeholder* e i principi del miglioramento continuo e dell'innovazione gestiti con regole, presidi e garanzie precise".

[5] Cfr. EUROPA 2020*. Una strategia per una crescita intelligente, sostenibile e inclusiva*. Bruxelles, 3 marzo 2010. COM (2010) 2020 definitivo. L'agenda 2020 definisce tre grandi priorità, fortemente connesse tra loro, da mettere in atto mediante azioni concrete a livello europeo e nazionale, per assicurare una crescita che sia: a) intelligente, ovvero capace di investire nei settori dell'istruzione, della ricerca e dell'innovazione; b) sostenibile, attenta alle politiche energetiche e rispettosa dei cambiamenti climatici; c) inclusiva, pronta a promuovere la coesione sociale e territoriale e a migliorare il mercato del lavoro.

integrazione sociale. A distanza di dieci anni dalla pubblicazione del Libro Verde, la Commissione Europea mediante la comunicazione del 25 ottobre 2011 (n. 681)[6], riesamina e supera la nozione espressa in precedenza offrendo una nuova definizione di responsabilità sociale d'impresa come "responsabilità delle imprese per il loro impatto sulla società". La nuova impostazione apporta significative novità alla complessa discussione intorno al tema, riducendo il peso di un approccio soggettivo delle imprese e richiedendo maggiore adesione ai principi promossi dalle organizzazioni internazionali. La Commissione Europea individua in tal modo un programma di azione affinché tutte le imprese europee adottino pratiche di responsabilità sociale in linea con i principi europei e internazionali, non solo per scopi puramente etici e di sostenibilità, ma anche in termini di vantaggi commerciali. A livello nazionale, di rimarchevole importanza assume l'art. 41 della Costituzione della Repubblica Italiana, contenuto nella Prima Parte *Diritti e Doveri dei cittadini*, Titolo II, *Rapporti economici*, mediante il quale il costituente ha voluto realizzare una

[6] Cfr. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Bruxelles, 25 ottobre 2011. COM (2011) 681 definitivo. La comunicazione concerne la strategia rinnovata dell'Unione Europea per il periodo 2011-2014 in materia di responsabilità sociale delle imprese. Programma d'azione: 1. Promozione della visibilità della RSI e diffusione di buone pratiche; 2. Miglioramento e monitoraggio dei livelli di fiducia delle imprese; 3. Miglioramento dei processi di autoregolamentazione e co-regolamentazione; 4. Aumento del premio di mercato per la RSI; 5. Migliore divulgazione da parte delle imprese delle informazioni sociale e ambientali; 6. Ulteriore integrazione della RSI nell'ambito dell'istruzione, della formazione e della ricerca; 7. Accentuazione dell'importanza delle politiche nazionali e sub-nazionali in materia di RSI; 8. Migliore allineamento degli approcci europei e globali alla RSI.

sintesi tra la libertà di iniziativa economica e la necessità che questa non sia assoluta, ma tenga conto dei limiti di legge e venga esercitata in un'ottica solidaristica[7]. L'articolo 41 costituzionale presenta un chiaro riferimento alla responsabilità sociale d'impresa, condizionando l'iniziativa economica privata al contributo che questa riesce a conferire all'utilità sociale e comunque non in nocumento alla sicurezza, libertà, e dignità umana[8]. È vero che l'imprenditore può avere soggettivamente un altro fine, quello strettamente egoistico, ma quello che è essenziale è riconoscere che l'impresa in sé è un'attività a finalità sociale[9]. Il decreto legislativo n. 81 del 9 aprile 2008 contiene la seguente definizione di "responsabilità sociale delle imprese: integrazione volontaria delle preoccupazioni sociali ed ecologiche delle aziende e organizzazioni nelle loro attività commerciali e nei loro rapporti con le parti interessate"[10]. A partire dal 2018, per la prima volta, circa

[7] Cfr. art. 41 COSTITUZIONE ITALIANA: "L'iniziativa economica privata è libera. Non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla sicurezza, alla libertà, alla dignità umana. La legge determina i programmi e i controlli opportuni perché l'attività economica pubblica e privata possa essere indirizzata e coordinata a fini sociali".

[8] JANNELLI R., MENEGUZZO M., FIORANI G. (2012), *CSR 2.0 proattiva e sostenibile. Tra mercati globali e gestione della crisi*, Egea, Milano, p. 208.

[9] COMPAGNONI F., ALFORD H. (2008), *Fondare la responsabilità sociale d'impresa. Contributi dalle scienze umane e dal pensiero sociale cristiano*, Città Nuova Editrice, Roma, p. 253.

[10] Cfr. art. 2, comma 1, par. ff del d.lgs. 9 aprile 2008, n. 81 - Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro. (GU Serie Generale n.101 del 30-04-2008 - Suppl. Ordinario n. 108). Per un approfondimento cfr. MURRU F. (a cura di) (2009), *Responsabilità sociale d'impresa. Il punto di vista dei lavoratori*, FrancoAngeli, Milano, p. 22 ss., il quale sostiene che "[…] alla prima lettura, si può notare che viene riportata solo la prospettiva delle aziende, mentre i lavoratori vengono

500 imprese italiane hanno dovuto presentare il rapporto sulla responsabilità sociale d'impresa assieme ai bilanci societari annuali di carattere economico-finanziario. Questo documento aggiuntivo è diventato obbligatorio quando il Governo tramite il decreto legislativo n. 254 del 30 dicembre 2016 ha attuato la direttiva 2014/95/UE sulla comunicazione di informazioni di carattere non finanziario e sulla diversità[11]. Secondo la normativa, solo le imprese di grandi dimensioni sono obbligate a presentare il rapporto: società quotate in borsa, banche, imprese assicurative e di riassicurazione e grandi gruppi, con un numero di almeno 500 dipendenti e uno dei due elementi seguenti: un bilancio consolidato in attivo superiore a 20 milioni di euro, o ricavi netti superiori ai 40 milioni di euro. La legge si basa sul principio che la responsabilità di un'impresa non si limita al valore dei beni e dei servizi che produce, ma include anche il suo impatto sulla società e l'ambiente naturale[12].

---

ricompresi marginalmente fra le parti interessate dai rapporti aziendali. […] Il capitale umano è il fulcro della RSI, ciò che la rende sostanza concreta. Un'impresa socialmente responsabile va oltre il semplice rispetto della normativa vigente, e, per farlo il primo investimento deve essere nel capitale umano. La conciliazione degli obiettivi economici con quelli sociali e ambientali produce effetti sulla società, quindi sulle persone. I beneficiari sono *in primis* i lavoratori stessi, che dovrebbero essere più motivati e fidelizzati da un clima aziendale che risente degli investimenti umani e sociali dell'azienda. Ma la ricaduta positiva va oltre i lavoratori, cioè raggiunge tutti i cittadini, che riconoscono una particolare credibilità e affidabilità al marchio aziendale […]".

[11] Decreto legislativo 30 dicembre 2016, n. 254. Attuazione della direttiva 2014/95/UE del Parlamento europeo e del Consiglio del 22 ottobre 2014, recante modifica alla direttiva 2013/34/UE per quanto riguarda la comunicazione di informazioni di carattere non finanziario e di informazioni sulla diversità da parte di talune imprese e di taluni gruppi di grandi dimensioni. (17G00002) (GU Serie Generale n.7 del 10-01-2017). Entrata in vigore del provvedimento: 25/01/2017.

[12] Il formato del *report* sulla RSI deve seguire linee guida e *standard* specifici. Le aree di rendicontazione previste dal d.lgs. n. 254 del 2016

## 3. Evoluzione storica del concetto di responsabilità sociale d'impresa nella letteratura manageriale

### *3.1 Le origini: anni Trenta, Quaranta e Cinquanta*

In letteratura è possibile trovare i primi riferimenti alla disciplina a partire dagli anni Trenta e Quaranta. Difatti, già nel 1938, Barnard evidenzia il ruolo sociale[13] delle imprese e l'importanza che riveste l'ambiente esterno nei processi decisionali del *management*. A distanza di quasi un decennio, Simon (1947) rimarca che le organizzazioni devono essere responsabili nei confronti della propria comunità di riferimento, al di là dei vincoli imposti dalla legge[14]. La prima definizione di responsabilità sociale

---

sono: 1) Ambiente. L'uso di energie rinnovabili, dell'acqua e di materiali riciclabili; emissioni di gas serra e inquinamento; 2) Impatto sulla società. I rapporti con le comunità locali e le iniziative per favorirne lo sviluppo; 3) Personale. Parità di genere, condizioni lavorative, sicurezza e salute sul luogo di lavoro, diritti sindacali, rispetto delle direttive ONU sul lavoro; 4) Diritti umani. Rispetto dei diritti umani, sia sul luogo di lavoro che nella *supply chain*; 5) Lotta alla corruzione. Iniziative per prevenire la corruzione attiva e passiva. Per ciascuna di queste aree, le imprese sono tenute a fornire informazioni rilevanti su: i modelli di *business* e di *management*; le politiche adottate; i rischi connessi; i miglioramenti rispetto agli anni precedenti. La legge cerca di trovare un equilibrio tra il dare delle chiare linee guida e lasciare spazio alla flessibilità. Il principio applicato è quello del *comply or explain*: le imprese possono tralasciare certe parti, a condizione però di spiegarne il motivo.

[13] BARNARD C. I. (1938), *The Functions of the Executive*, Cambridge MA, Harvard University Press. Il volume presenta una teoria della cooperazione e dell'organizzazione e uno studio delle funzioni e dei metodi di funzionamento dei dirigenti nelle organizzazioni formali.

[14] SIMON H. A. (1947), *Administrative Behaviour: A Study of the Decision Making Processes in Administrative Organisation*, New York, Macmillan Company. È considerato uno dei punti di riferimento

d'impresa[15] viene fornita nel 1953 da Bowen. La *Corporate Social Responsibility* (CSR) "si riferisce agli obblighi dei *businessmen* a seguire quelle politiche, a prendere quelle decisioni, o a portare avanti quelle linee di azione che sono desiderabili in termini di obiettivi e valori della nostra società"[16]. L'autore dà una definizione di responsabilità sociale riferita al *businessman*, come responsabilità individuale di *manager*. Secondo la sua visione, le imprese sono riconosciute come centri vitali di potere in grado di condizionare la società. Drucker (1954) è il primo autore che adopera l'espressione *social responsabilities of business*. A differenza di Barnard (1938) e Simon (1947), che attribuiscono maggiore enfasi alle dimensioni etiche e morali del comportamento degli individui all'interno delle organizzazioni, Drucker si sofferma sulla responsabilità del soggetto collettivo:

---

nell'evoluzione della teoria delle decisioni. L'autore sostiene che il comportamento decisionale nell'organizzazione è volutamente razionale e che le decisioni sono prese da individui all'interno di organizzazioni e non da organizzazioni come entità. Ha anche riconosciuto l'inadeguatezza della teoria classica per la comprensione delle decisioni nelle organizzazioni. Di conseguenza, ha distinto il ruolo dei fatti e il ruolo dei valori nel processo decisionale.

[15] Nel 1953, su invito di un'assemblea di chiese protestanti, l'economista Howard Bowen, seguace dell'istituzionalismo di J. R. Commons ed estimatore dell'approccio socio-antropologico di Karl Polanyi, esegue il primo studio ad ampio raggio sulla formazione di una coscienza sociale nei *businessmen*, arrivando a dare un'impostazione già matura e organica a dei problemi ancora oggi discussi negli studi di *Corporate Social Responsibility* (CSR). Lo sfondo storico da cui le sue riflessioni muovono è quello della Depressione e poi della rinascita economica negli anni della Seconda Guerra Mondiale. Cfr. l'ampia riflessione di MORRI L. (2009), *Storia e teorie della responsabilità sociale d'impresa. Un profilo interpretativo*, FrancoAngeli, Milano, p. 15 ss.

[16] BOWEN H. R. (1953), *Social responsibilities of the businessmen*, New York, Harper & Row.

l'impresa[17]. La *public responsibility* è uno degli otto obiettivi primari che l'impresa deve prefiggersi. Quando il *management* agisce "è necessario valutare se l'azione intrapresa possa servire a promuovere il bene pubblico, a far progredire i valori di base della nostra società, a contribuire alla sua stabilità, alla sua forza e alla sua armonia"[18]. Sulla stessa direttrice degli studi di Drucker vi è il contributo di Selznick (1957), il quale sostiene che le imprese, per poter affrontare i problemi insiti nella società (cosa da cui non si possono esimere, essendone protagoniste) debbono prefiggersi degli obiettivi che non sono esclusivamente di natura economica[19]. Altro contributo meritevole di menzione è quello di Heald (1957) che definisce la CSR come "il riconoscimento da parte del *management* di un obbligo nei confronti della società. Serve non solo per il massimo rendimento economico ma anche per politiche sociali e umane"[20]. Levitt (1958) prende posizioni contrastanti rispetto agli altri autori. Egli accusa la CSR di rappresentare un potenziale pericolo per le fondamenta del libero mercato e di offuscare il ruolo delle imprese e del Governo nazionale[21].

---

[17] Cfr. NIGRO C., PETRACCA M. (2016), *La CSR dalle origini all'approccio neo-istituzionalista. Focus sui processi di isomorfismo e di decoupling*, G. Giappichelli Editore, Torino, p. 11.

[18] DRUCKER P. F. (1954), *The practice of management*, New York, Harper & Row Publishers, p. 388.

[19] SELZNICK P. (1957), *Leadership in Administration: a Sociological Perspective*, New York, Harper & Row Publishers.

[20] HEALD M. (1957), *Management's Responsibility to Society: The Growth of an Idea*, Business History Review, 31(4), 375-384, p. 380.

[21] LEVITT T. (1958), *The Dangers of Social Responsibility*, Harvard Business Review, 36, 41-50. A pag. 47, op. cit., l'autore prende posizione affermando che "il lavoro del Governo non è il *business* e il lavoro delle imprese non è il Governo".

### *3.2 Gli anni Sessanta: l'affermazione del principio di volontarietà*

L'esistenza di uno stretto nesso[22] tra potere e responsabilità sociale delle imprese si afferma nel 1960 con la *Iron Law of Responsibility*, postulata da Davis, secondo cui la inadeguata attenzione verso l'esterno da parte dell'impresa porta a una progressiva corrosione del potere della stessa, danneggiandone di conseguenza la redditività, se non la stessa sopravvivenza. Secondo questa prospettiva, dunque, poiché responsabilità e potere sono destinati a equilibrarsi costantemente, la diminuzione dell'una reca con sé quella dell'altra[23]. La questione della relazione tra impresa e *claimants*[24] si pone nella conferenza *The Social Responsibility of Marketing* (1960). Nello stesso anno Frederik designa una definizione di CSR più completa che mette in rilievo la funzione sociale di creazione di benessere, che va al di là della dimensione economica, con finalità più ampie rispetto a interessi circoscritti di persone e imprese[25]. La definizione viene ampliata nel 1963 da

---

[22] DAVIS K. (1960), *Can business afford to ignore social responsibilities?*, California Management Review, 2(3), 70-76. Cfr. op. cit. p. 73 "[…] il rifiuto della responsabilità sociale conduce ad una graduale erosione del potere sociale nella misura in cui i *businessmen* non accettano le opportunità della responsabilità sociale che sopraggiungono, altri gruppi si faranno avanti per assumere queste responsabilità. Nella storia, governo e sindacati sono stati i più attivi nel compito di diluire il potere dell'impresa, e continueranno probabilmente ad essere i principali soggetti sfidanti".

[23] Cfr. DAVIS K. (1967), *Understanding the Social Responsibility Puzzle*, Business Horizons, 10(4), 45-50.

[24] Cfr. SCIARELLLI S., SCIARELLI M. (2018), *Il governo etico d'impresa*, Cedam, Padova, p. 50. I *claimants*, secondo gli autori, sono gli aventi diritto verso i quali l'impresa assume obblighi di diversa natura.

[25] FREDERIK W. C. (1960), *The growing concern over business responsibility*, California Management Review, 2(4), 54-61.

McGuire[26], secondo cui le imprese devono occuparsi del benessere della comunità e della felicità dei dipendenti, operando "come dovrebbe un vero cittadino"[27]. La definizione di RSI viene rivista da Davis e Blomstrom (1966) come "gli obblighi di una persona di considerare gli effetti delle sue decisioni e delle sue azioni sull'intero sistema sociale. Il *businessman* applica la responsabilità sociale quando considera che i bisogni e gli interessi degli altri possono essere intaccati dalle azioni dell'impresa. Così facendo egli va oltre i confini economici e tecnici dell'impresa"[28]. Solo nel 1967 Walton evidenzia l'esistenza di un *link* intimo tra società e impresa[29]. In sostanza, l'autore dichiara che la responsabilità sociale

[26] MCGUIRE J. W. (1963), *Business and Society*, New York, McGraw Hill. A pag. 144, op. cit., l'autore afferma che "l'idea della responsabilità sociale suppone che l'impresa non ha solo obblighi economici e legali, ma anche alcune responsabilità verso la società che vanno oltre tali obblighi".

[27] È la prima idea da cui si svilupperà in seguito il concetto di *Corporate Citizenship* secondo il quale l'impresa è, al pari di un individuo, portatrice di un *set* di diritti e di responsabilità che la rendono interdipendente con gli altri attori della comunità di riferimento. L'impresa ha un ruolo sociale per cui: a) non fa parte solo del patrimonio del proprietario legale degli *asset*, ma di tutti quelli che partecipano al loro sfruttamento; b) facendo sostenere costi alla società, ha anche delle responsabilità e dei doveri nei suoi confronti. Cfr. sul tema CARROLL A. B. (1998), *The four faces of corporate citizenship*, Business and Society Review, 100(1), 1-7.

[28] DAVIS K., BLOMSTROM R. L. (1966), *Business and its Environment*, New York, McGraw Hill, p. 12.

[29] WALTON C. C. (1967), *Corporate social responsibilities*, Belmont, Wadsworth Publishing Company, p. 18. Secondo l'autore, gli elementi alla base della CSR sono: 1) un tasso di volontarietà da parte dell'impresa; 2) un indiretto collegamento tra alcune organizzazioni volontarie e le imprese; 3) l'accettazione che per i costi sostenuti non sempre è possibile misurare a priori i possibili ritorni economici associati.

deve essere considerata un processo di attuazione volontario e non coercitivo, sia da parte dei *manager* che da parte dell'impresa. Detto altrimenti, si afferma dunque il principio della volontarietà della responsabilità sociale, in cui la gestione responsabile delle istanze che provengono dalla società è una scelta volontaria che non può essere obbligata dalla legge[30].

### *3.3 Gli anni Settanta: le varie declinazioni e categorie*

Nel 1971 Johnson individua e chiarisce le definizioni presenti fino a quel momento in letteratura[31]. Egli individua quattro possibili declinazioni della CSR: 1. "saggezza convenzionale", 2. "massimizzazione dei profitti di lungo periodo", 3. "massimizzazione dell'utilità", 4. "visione

[30] Cfr. sul tema i contributi di MANNE H. G., WALLICH H. C. (1972), *The modern corporation and social responsibility*, Washington, American Enterprise Institute for Public Policy Research; DAVIS K. (1973), *The case for and Against Business Assumption of Social responsibilities*, The Academy of Management Journal, 16(2), 312-322.

[31] JOHNSON H. L. (1971), *Business in contemporary society: Framework and issues*. Belmont CA, Wadsworth Pub. Co., pp. 50-77. Secondo l'attenta riflessione di NIGRO C., PETRACCA M. (2016), *La CSR dalle origini all'approccio neo-istituzionalista. Focus sui processi di isomorfismo e di decoupling*, G. Giappichelli Editore, Torino, p. 16 ss. in merito alle quattro declinazioni della CSR proposte da JOHNSON H. L. (1971), op. cit., la (1) "saggezza convenzionale" corrisponde a una sorta di bilanciamento da parte dei *manager* di una molteplicità di interessi diversi; quanto alla (2) "massimizzazione dei profitti di lungo periodo", le imprese intraprendono programmi sociali al fine di incrementare il profitto; (3) la "massimizzazione dell'utilità" rilancia la figura del *manager*/imprenditore socialmente responsabile interessato non solo al proprio benessere ma anche a quello della comunità; in ultimo, secondo la (4) "visione lessicografica della responsabilità sociale", gli obiettivi della impresa come pure quelli degli individui sono classificati in ordine di importanza.

lessicografica della responsabilità sociale". Eilbirt e Parket (1973) si soffermano sull'implementazione pratica della CSR. Definita dagli autori come "l'impegno di un *business*, o del *business* in generale, ad un ruolo attivo nella soluzione dei problemi sociali in senso ampio, come la discriminazione razziale, l'inquinamento, i trasporti o il degrado urbano", è costituita da una pluralità di differenti attività ed è associata a variabili organizzative[32]. Sethi (1975) studia le attività di *corporate social performance* e le classifica in tre diverse categorie: 1. *social obligations*, cioè comportamenti aziendali in risposta alle forze di mercato o agli impedimenti legali; 2. *social responsibility* che implicano comportamenti aziendali fino ad un livello che sia congruente con le prevalenti norme sociali, valori e aspettative; 3. *social responsiveness*, che implicano un adattamento preventivo dei comportamenti aziendali ai bisogni della società[33]. Secondo Fitch (1976), la CSR è delineata in termini di risoluzione di problemi sociali e definita come "una serie di tentativi tesi a trovare soluzioni a problematiche sociali causate interamente o in parte da azioni intraprese dalle imprese". Le imprese devono identificare e definire un problema sociale, decidere come aggredirlo e, infine, quale soluzione attuare. Fondamentale è la capacità di identificare i metodi per affrontare le questioni sociali[34]. Ackerman e Bauer (1976) sostengono che il termine *social responsibility* enfatizza solo le motivazioni e non le *performance*; dunque, meglio parlare di *social responsiveness*, ovvero di sensibilità e attenzione

[32] EILBIRT H., PARKET R. (1973), *The practice of business: The current status of corporate social responsibility*, Business Horizons, 16(4), 5-14.

[33] Cfr. SETHI S. P. (1975), *Dimensions of Corporate Social Performance: An Analytical Framework*, California Management Review, 17(3), 58-64.

[34] FITCH H. G. (1976), *Achieving Corporate Social Responsibility*, Academy of Management Review, 1(1).

verso le istanze sociali, focalizzandosi su scelte aziendali in grado di anticipare tali problematiche sociali[35]. Il carattere statico e prettamente teorico della *Corporate Social Responsibility* ($CSR_1$) viene superato da Frederick nel 1978, il quale identifica la *Corporate Social Rensponsiveness* ($CSR_2$)[36]. Secondo Frederick (1994), per *Corporate Social Rensponsiveness* si intende la capacità di risposta manageriale pratica alle pressioni sociali. In altri termini, si tratta di pratiche manageriali per mettere in atto la gestione responsabile, attraverso l'analisi delle istanze provenienti dalla società e dai diversi interlocutori. Una teoria più completa e ampia si inizia a definire nel 1979 grazie al contributo di Carroll, il cui modello a quattro stadi della responsabilità sociale[37] segna un passaggio fondamentale nello sviluppo della ricerca. Il modello in questione prevede che l'impresa abbia quattro tipologie di responsabilità, che verranno successivamente poste dallo stesso autore in ordine gerarchico crescente: economiche, giuridiche, etiche, discrezionali[38]. Il modello della Piramide della Responsabilità Sociale d'Impresa pone al primo stadio le responsabilità di creare valore economico per gli azionisti e valore in termini di offerta di beni e servizi per il mercato (*be profitable*). Quanto alla responsabilità legale (*obey the law*), posta al secondo

[35] ACKERMAN R., BAUER R. A. (1976), *Corporate Social Responsiveness: Modern Dilemma*, Reston VA, Reston Publishing Company.

[36] Il contributo di Frederick del 1978 è un *working paper* dell'Università di Pittsburgh, pubblicato nel 1994. Cfr. FREDERICK W. C. (1994), *From $CSR_1$ to $CSR_2$: The maturing of business-and-society thought*, Business & Society, 33(2), 150-164.

[37] CARROLL A. B. (1979), *A three-dimensional conceptual model of corporate performance*, Academy of Management Review, 4(4), 497-505.

[38] CARROLL A. B. (1991), *The pyramid of corporate social responsibility: Toward the moral management of organizational stakeholders*, Business Horizons, 34(4), 39-48.

livello, le imprese si impegnano a rispettare le leggi che la società richiede. La responsabilità etica (*be ethical*), ossia la conformità al sistema di princìpi, valori e norme sociali (equità, giustizia, imparzialità) e la responsabilità filantropica (*be a good corporate citizen*), vale a dire l'impegno da parte dell'impresa in investimenti a favore della comunità, sono entrambe volontarie. Jones sostiene che la CSR si basa sul riconoscimento di obblighi rispettati volontariamente dall'impresa non soltanto verso gli azionisti, ma anche verso i lavoratori, i fornitori, i consumatori e le comunità locali. Secondo l'autore, la CSR è dunque un processo (e non una serie di risultati) che richiede azioni finalizzate alla sua implementazione e i processi di *decision making* finalizzati alla CSR costituiscono la base di comportamenti socialmente responsabili[39].

### *3.4 Gli anni Ottanta: la teoria degli stakeholder e la business ethics*

Negli anni Ottanta gli studi in materia si moltiplicano e nascono due filoni di letteratura: 1. la Teoria degli *Stakeholder* e 2. gli studi di *Business Ethics*. Grazie al contributo di Freeman del 1984 nasce la teoria degli *stakeholder*[40]: si tratta di studi orientati all'analisi e

[39] JONES T. M. (1980), *Corporate Social Responsibility Revisited, Redefined*, California Management Review, 22(3), 59-67.

[40] FREEMAN R. E. (1984), *Strategic Management: A Stakeholder Approach*, Boston, Pitman. Il termine *stakeholder* è elaborato nel 1963 al *Research Institute* dell'Università di Stanford. Gli *stakeholder* sono "individui o gruppi di individui che sono influenzati o che possono influenzare il raggiungimento degli obiettivi di impresa". Vengono distinti da CLARKSON M. B. E. (1995), *A Stakeholder Framework for Analyzing and Evaluating Corporate Social Performance*, The Academy

all'approfondimento della gestione strategica d'impresa, nell'ottica di massimizzare non solo il valore per gli azionisti ma il benessere di tutti gli *stakeholder*. Questi studi partono dall'idea che nel lungo periodo risultati equilibrati e favorevoli per la complessità degli *stakeholder* rappresentano una garanzia di sopravvivenza e benessere maggiore rispetto a strategie rivolte alla massimizzazione dei risultati unicamente destinati agli azionisti. Gli studi di *Business Ethics* invece, concentrati sul versante morale, hanno favorito la nascita di due distinte visioni della RSI[41]: (a) la visione strategica, la quale individua il sorgere di un certo tipo di vantaggio economico dal perseguimento di finalità sociali da parte dell'impresa, e (b) la visione etica che, ravvedendo una sorta di dovere dell'impresa ad agire correttamente senza danneggiare alcun soggetto, ritiene che tale agire debba essere perpetrato anche se non necessariamente vantaggioso[42]. Di rimarchevole importanza il contributo di Frederick (1986), secondo il

---

of Management Review, 20(1), 92-117 in primari e secondari, in funzione dell'indispensabilità o meno del loro apporto alla sopravvivenza dell'impresa. Sono *stakeholder* primari gli azionisti, i dipendenti, i clienti e i fornitori; sono *stakeholder* secondari i *mass media*, i movimenti d'opinione e di difesa del cittadino, i gruppi sociali, le associazioni locali e le associazioni speciali.

[41] Altri contributi più recenti, nell'ambito degli studi dell'etica d'impresa, offrono ulteriori spunti di analisi per i collegamenti con la teoria degli *stakeholder*. Cfr., ad es., la teoria del contratto sociale integrativo di DONALDSON T., DUNFEE T. W. (1994), *Toward a unified conception of business ethics: Integrative social contracts theory*, Academy of Management Review, 19(2), 252-284; DUNFEE T. W., DONALDSON T. (1999), *Social Contract Approaches to Business Ethics: Bridging the "Is-Ought" Gap* in FREDERICKS R. (a cura di), *A companion to business ethics*, Oxford, Blackwell, pp. 38-55 e la teoria della cittadinanza di MCGUIRE J. W. (1963), op. cit.

[42] JEURISSEN R. (2000), *John Elkington, Cannibals With Forks: The Triple Bottom Line of 21st Century Business*, Journal of Business Ethics, 23(2), 229-231.

quale nell'evoluzione degli studi sulle relazioni tra società e *business* si individuano tre correnti di pensiero: 1. $CSR_1$, focalizzata sul concetto di *corporate social responsibility*, che sostiene che le imprese si debbano impegnare per il benessere della società; 2. $CSR_2$, incentrata sulla *corporate social responsiveness*, si basa sul tentativo di comprendere quali azioni e quali strumenti l'impresa deve adottare per fronteggiare le pressioni sociali; 3. $CSR_3$, incentrata sulla *corporate social rectitude*, che si riflette nella nozione di correttezza morale nelle azioni intraprese e nelle politiche formulate, ed è connessa ad una radicata *culture of ethics*[43].

### *3.5 Gli anni Novanta: verso la sostenibilità e la rendicontazione sociale*

Negli anni Novanta si sviluppa una nuova e diversa attenzione ai temi della RSI. Le principali direzioni di approfondimento sono due: 1. analisi dei rendimenti associati a fondi che investono in imprese selezionate in base a criteri etici (finanza sostenibile); 2. studi incentrati sulle *performance* della singola impresa che adotta comportamenti socialmente responsabili. In aggiunta, si sviluppano gli studi relativi alla rendicontazione sociale, intesa sia come elemento di congiunzione fra azioni

[43] FREDERICK W.C. (1986), *Toward $CSR_3$: Why Ethical Analysis is Indispensable and Unavoidable in Corporate Affairs*, California Management Review, 28(2), 126-141. Caratteristiche dell'impresa allineata alla $CSR_3$: a) considera le questioni etiche come aspetti *core* e non periferici nelle scelte e politiche manageriali; b) impiega esclusivamente *manager* che attribuiscono una posizione predominante all'etica in tutte le loro operazioni di gestione quotidiane; c) è dotata di strumenti d'analisi sofisticati per scovare e anticipare le problematiche etiche afferenti all'impresa e ai suoi dipendenti; d) cerca di allineare le politiche aziendali correnti e future con i valori tipici di una cultura basata sull'etica.

compiute e risultati ottenuti, sia come strumento di valorizzazione delle sinergie fra responsabilità sociale e *performance* realizzate. Inoltre, si accentua la consapevolezza dell'emergenza ambientale e l'attenzione alla tutela degli ecosistemi e delle risorse naturali. Le motivazioni illustrate da Wood (1991) che spingono l'impresa a comportamenti responsabili possono essere ricondotte a tre dimensioni: istituzionale, organizzativa, individuale[44]. Si afferma l'approccio *Triple Bottom Line* (1994), «economico, sociale, ambientale», al cui centro è posto il tema della sostenibilità[45]. Frederick (1998) offre la

[44] WOOD D. J. (1991), *Corporate social performance revisited*, Academy of Management Review, 16(4), 691-718. Secondo l'attenta riflessione di SCIARELLI S., SCIARELLI M. (2018), *Il governo etico d'impresa*, Cedam, Padova, p. 52. in merito al saggio di WOOD D. J. (1991), "[…] l'impresa viene spinta ad essere responsabile come istituzione che opera in una società e che non vuole perdere la propria legittimazione. L'impresa è un sistema organizzato che ha una responsabilità pubblica per la soluzione dei problemi che causa direttamente o indirettamente. L'impresa è guidata da uomini, che hanno i loro principi etici, che li indirizzano nelle scelte discrezionali, volte a soddisfare interessi di interlocutori, delle quali si assumono perciò una responsabilità in termini di conseguenze".

[45] ELKINGTON J. (1994), *Towards the Sustainable Corporation: Win-Win-Win Business Strategies for Sustainable Development*, California Management Review, 36(2), 90-100. Secondo una concezione oramai consolidata, la RSI si caratterizza per l'impegno assunto dall'impresa secondo l'approccio "*Triple Bottom Line*" o "Triplice approccio". Tale concetto venne introdotto per la prima volta dal sociologo ed economista inglese John Elkington con la sua *Sustainability Ltd*. Si tratta di un approccio basato sulla triplice dimensione dell'attività economica di un'impresa che sottende non solo il raggiungimento del profitto, ma anche il rispetto dei diritti dei lavoratori e della comunità, nonché la tutela dell'ambiente. La Commissione Europea ha definito il "Triplice approccio" come la "concezione secondo la quale le prestazioni globali di un'impresa devono essere misurate in funzione del suo contributo combinato alla prosperità, alla qualità dell'ambiente e al capitale sociale". Rifacendosi a questa definizione, la sostenibilità è valutata

secondo tre direttrici: quella economica, per cui si fa riferimento alla capacità di generare ricchezza e, quindi, di assicurare la sopravvivenza e lo sviluppo dell'impresa; quella sociale, da intendersi quale responsabilità nei confronti dei vari soggetti interni ed esterni all'organizzazione; quella ambientale, nel senso di attenzione all'equilibrio ecologico. L'imprenditore, secondo tale metodo, dovrà optare per politiche di sviluppo che bilanciano correttamente le tre direttive e si pongono come punto di equilibrio fra queste. Il bilanciamento ottimale per garantire lo sviluppo di lungo periodo dell'impresa, pertanto, non è quello che assicura meccanicamente nell'immediato il maggior profitto possibile. Anzi, nel breve periodo, potrà derivarne anche un decremento degli utili economici dell'impresa, in quanto è nel lungo periodo che la scelta del bilanciamento ottimale garantirà all'impresa quel consenso sociale che la porrà a riparo da iniziative di boicottaggio a livello globale da parte dei consumatori o da atteggiamenti di ostilità dei pubblici poteri. Il primario obiettivo dell'imprenditore, pertanto, rimarrà indiscutibilmente il conseguimento del massimo risultato economico, ma l'imprenditore avveduto - coerentemente alla "*Triple bottom line*" - dovrà scegliere di perseguire tale obiettivo impiegando strategicamente la RSI quale elemento di valorizzazione e differenziazione competitiva della propria attività. Adottare volontariamente comportamenti responsabili consentirà, difatti, di rispondere adeguatamente alle istanze degli *stakeholders* ponendo, per tale via, le basi per uno sviluppo duraturo della propria impresa. La conseguenza di una gestione basata sulla *Triple Bottom Line* ha anche ulteriori ripercussioni. Essa fa nascere nella mentalità imprenditoriale la consapevolezza di dover leggere i fenomeni aziendali sotto "lenti" diverse da quelle solitamente utilizzate per la contabilità generale basata sul sistema dei prezzi, cercando di far emergere da ogni scelta imprenditoriale e da ogni transazione il relativo valore sociale, economico ed ambientale. Acquisito, oramai, che la RSI si sviluppa nelle due direttrici sociali ed ambientali, si deve ribadire nuovamente come, sino ad oggi, la dottrina abbia mostrato maggior attenzione alle tematiche sociali piuttosto che a quelle ambientali, creando un modello di RSI in cui la categoria ambientale costituisce chiaramente un sottoinsieme di quella sociale. Con la comunicazione n. 347 del 2 luglio del 2002, la Commissione Europea ha sollecitato le grandi imprese quotate a pubblicare ogni anno la "*Triple Bottom Line*" *Reporting*, una

definizione della $CSR_4$, la *corporate social reason*, che riassume i diversi contributi esistenti in materia di CSR e propone il superamento dell'idea che l'impresa è al centro del mondo e che attorno ruotano le altre istituzioni, per mettere al centro la società e l'ambiente. Lo studio delle *social issue* nel *management* deve essere svolto su un nuovo livello, quello delle scienze naturali, nella prospettiva cosmologica, evoluzionista e del naturalismo. Fare $CSR_4$ vuole dire affrontare il tema della sostenibilità economica, sociale e ambientale[46].

### *3.6 Il nuovo millennio: la corporate sustainability e il valore condiviso*

Negli ultimi due decenni l'attenzione si è spostata dalla convenienza economica della RSI verso la più ampia tematica che collega un atteggiamento dell'impresa socialmente responsabile alla soddisfazione di tutti gli *stakeholder*, elemento imprescindibile per il successo

---

forma di bilancio finalizzata a tenere informati gli azionisti sul proprio impegno nel bilanciamento di questi tre elementi: protezione ambientale, responsabilità sociale e prosperità economica, o come vengono più comunemente chiamati, 3Ps (*people*, *planet and profits*). L'adesione al *TBL Approach* rappresenta il passaggio alla nuova economia, sempre più incentrata al benessere della collettività e dell'ambiente più che solo al mero profitto. Quando un'impresa riesce a soddisfare, parimenti, le necessità di tutte e tre le categorie senza che ci sia prevaricazione di una sull'altra, allora quell'impresa potrà dire di essere riuscita a sintetizzare il vero concetto di sostenibilità, promuovendo un'idea di sviluppo che non mette a rischio le condizioni di vita per le future generazioni. Cfr. MERLI R. (2012), *La responsabilità sociale d'impresa: aspetti teorici e strumenti operativi*, Cedam, Padova, passim.

[46] FREDERICK W. C. (1998), *Moving to CSR4: what to pack for the trip*, Business and Society, 37(1), 40-59.

dell'impresa e dunque si evidenzia una più matura interpretazione della positività dei risultati aziendali in un'ottica di soddisfazione degli *stakeholder*. Obiettivo degli studi non è solo dimostrare la convenienza economica della RSI, quanto piuttosto chiarire quali fattori ne giustificano l'esistenza, per fornire elementi utili per un proficuo raggiungimento e una corretta gestione della stessa. Quanto ai destinatari, non solo esponenti della comunità scientifica, ma anche operatori economici (in particolare i vertici aziendali), che riconoscono l'utilità dei risultati ottenuti. Emerge nell'ultimo decennio l'articolo di Porter e Kramer (2011), nel quale sostengono che il sistema capitalistico è sotto assedio, perché l'opinione pubblica considera l'operato delle grandi aziende come la causa principale dei problemi sociali, ambientali ed economici[47]. La soluzione proposta alle imprese è l'adozione di politiche mirate alla produzione di *Shared Value* (SV) o Valore Condiviso, definito dagli autori come l'insieme delle politiche e delle pratiche operative che rafforzano la competitività di un'azienda, migliorando nello stesso tempo le condizioni economiche e sociali delle comunità in cui opera[48]. Più in generale, nell'ultimo decennio sono nate

[47] PORTER M. E., KRAMER M. R. (2011), *The Big Idea: Creating Shared Value. How to Reinvent Capitalism—and Unleash a Wave of Innovation and Growth*, Harvard Business Review, 89(1-2), 62-77.

[48] *Creating shared value* (CSV) è un concetto di *business* introdotto per la prima volta nell'articolo di PORTER M. E., KRAMER M. R. (2006), *Strategy & Society: The Link between Competitive Advantage and Corporate Social Responsibility* pubblicato in Harvard Business Review. Vincitore del *McKinsey Award* per il miglior articolo di *Harvard Business Review* nel 2006, superando i principi generici di RSI, scoprì come l'influenza della società sta diventando la nuova frontiera del vantaggio competitivo. Il concetto è stato ulteriormente ampliato nel pezzo di *follow-up* del gennaio 2011 intitolato "*Creating Shared Value: Redefining Capitalism and the Role of the Corporation in Society*". Scritto da Michael E. Porter, una delle principali autorità sulla strategia

nuove tendenze delle imprese in materia di CSR[49]: nell'industria 4.0 è cambiato il modo di lavorare, sono nate nuove figure professionali e sono cambiati ruoli e gerarchie[50]. Per fare fronte alle nuove sfide del mercato, la sostenibilità deve essere quindi integrata nel modello di *business* e pertanto richiede un salto culturale nel *mindset* e nei comportamenti, un cambiamento necessario per essere competitivi e mantenere valore nel lungo periodo: si fa particolare riferimento alla *Corporate Sustainability*

---

competitiva e capo dell'Istituto per la strategia e la competitività presso la *Harvard Business School*, e Mark R. Kramer, *Kennedy School* presso l'Università di Harvard e co-fondatore di FSG, l'articolo fornisce approfondimenti ed esempi rilevanti di aziende che hanno sviluppato legami profondi tra le proprie strategie aziendali e la responsabilità sociale d'impresa. Nel 2012, Kramer e Porter, con l'aiuto della società di consulenza globale senza scopo di lucro FSG, hanno fondato la *Shared Value Initiative* per migliorare la condivisione delle conoscenze e la pratica relativa alla creazione di valore condiviso, a livello globale. La premessa centrale alla base della creazione di valore condiviso è che la competitività di un'azienda e il benessere delle comunità che la circondano sono reciprocamente dipendenti. Riconoscere e trarre vantaggio da queste connessioni tra progresso sociale ed economico ha il potere di scatenare la prossima ondata di crescita globale e di ridefinire il capitalismo. I critici, d'altra parte, sostengono che "Porter e Kramer raccontano fondamentalmente la vecchia storia della razionalità economica come l'unico e unico strumento di gestione intelligente, con fiducia nell'innovazione e nella crescita, e celebrano un capitalismo che ora ha bisogno di aggiustarsi un poco". Altri considerano le argomentazioni degli autori come un "approccio da *pony* con un solo trucco" con poche possibilità che una società civile sempre più critica possa accettare una simile storia. Cfr. BESCHORNER T. (2013), *Creating Shared Value: The One-Trick Pony Approach*, Business Ethics Journal Review, 1(17), 106–112.

[49] NIGRO C., PETRACCA M. (2016), *La CSR dalle origini all'approccio neo-istituzionista. Focus sui processi di isomorfismo e di decoupling*, G. Giappichelli Editore, Torino, p. 36 ss.

[50] SCARCELLA PRANDSTRALLER S. (a cura di) (2013), *Teorie e tecniche della responsabilità sociale d'impresa*, Di Virgilio Editore, Roma, passim.

(CS). La *Corporate Sustainability* è un approccio che mira a creare valore per gli *stakeholder* a lungo termine attraverso l'attuazione di una strategia aziendale incentrata sulle dimensioni etiche, sociali, ambientali, culturali ed economiche del fare impresa. Le strategie create hanno lo scopo di promuovere la longevità, la trasparenza e il corretto sviluppo dei dipendenti all'interno delle organizzazioni aziendali[51]. La CS viene spesso confusa con la CSR, sebbene le due non siano esattamente la stessa cosa[52]. È la nozione di "tempo" che discrimina la sostenibilità dalla RSI e altri concetti simili. Mentre l'etica, la moralità e le norme permeano la RSI, la sostenibilità obbliga solo le imprese a fare compromessi intertemporali per salvaguardare l'equità intergenerazionale[53]. È dunque il breve termine la rovina della sostenibilità[54].

---

[51] ASHRAFI M., ACCIARO M., WALKER T. R., MAGNAN G. M., ADAMS M. (2019), *Corporate sustainability in Canadian and US maritime ports*, Journal of Cleaner Production, 220, 386-397.

[52] ASHRAFI M., ADAMS M., WALKER T. R., MAGNAN G. M. (2018), *How corporate social responsibility can be integrated into corporate sustainability: a theoretical review of their relationships*, International Journal of Sustainable Development & World Ecology, 25 (8), 672-682.

[53] L'equità intergenerazionale in contesti economici, psicologici e sociologici è il concetto o l'idea di equità o giustizia tra generazioni. Il concetto può essere applicato all'equità nelle dinamiche tra bambini, giovani, adulti e anziani, in termini di trattamento e interazioni. Può anche essere applicato all'equità tra le generazioni attualmente viventi e le generazioni che devono ancora nascere. Le conversazioni sull'equità intergenerazionale avvengono in diversi campi. Viene spesso discusso in economia pubblica, specialmente per quanto riguarda l'economia di transizione, la politica sociale e la definizione del bilancio del governo. L'equità intergenerazionale viene esplorata anche nelle questioni ambientali, compreso lo sviluppo sostenibile, il riscaldamento globale e il cambiamento climatico.

[54] BANSAL P., DESJARDINE M. R. (2014), *Business sustainability: It is about time*, Strategic Organization, 12(1), 70-78.

## 4. Marketing socialmente responsabile: strategia d'impresa e misurazione della performance

La mercatistica (o mercatologia) è la disciplina aziendale più fortemente interessata al collegamento tra le imprese e gli ambienti in cui operano[55]. La responsabilità sociale delle imprese è stata discussa in modo frammentato nel contesto della disciplina del *marketing*. Alcune importanti scuole di pensiero della disciplina hanno incoraggiato la generazione di teorie sulla RSI e molti contributi sono stati limitati a determinate dimensioni del costrutto. Al contrario, nella letteratura manageriale si trovano numerosi studi teorici e sforzi di categorizzazione relativi alla RSI, che limitano il *marketing* a poche ma valide valutazioni di prospettive teoriche. Gli studiosi della disciplina si sono concentrati inizialmente sull'ampliamento dei concetti di *marketing* e hanno analizzato le funzioni sociali della impresa per poi concentrarsi sulle modalità strategiche di applicazione della RSI; nella maggior parte dei casi si sono concentrati sui principali *stakeholder* dell'impresa: consumatori e canali di distribuzione[56]. Dato il clima di sfiducia a causa di scandali, le imprese tendono sempre di più a dichiararsi socialmente responsabili, applicando iniziative strategiche nella propria gestione[57].

---

[55] VAALAND T., HEIDE M., GRONHAUG K. (2008), *Corporate social responsibility: Investigating theory and research in the marketing context*, European Journal of Marketing, 42(9/10), 927-953.

[56] SANCLEMENTE-TÉLLEZ J. C. (2017), *Marketing and Corporate Social Responsibility (CSR). Moving between broadening the concept of marketing and social factors as a marketing strategy*, Spanish Journal of Marketing – ESIC, 21(1), 4-25. L'articolo mette in relazione il concetto di RSI con il *marketing*, presentando una classificazione delle diverse prospettive teoriche secondo cui questi due costrutti sono correlati.

[57] MAIGNAN I., FERRELL O. C. (2004), *Corporate social responsibility and marketing: An integrative framework*, Journal of the Academy of Marketing Science, 32(1), 3-19.

### *4.1 La strategia d'impresa*

Un numero crescente di imprese in tutto il mondo sta abbracciando la RSI e sente la necessità di comprenderne meglio il significato e la portata, nonché le sue relazioni con il *marketing*. Le azioni di RSI stanno progressivamente diventando questioni aziendali di massima priorità e le imprese stanno implementando diverse iniziative che cercano di dare un senso al concetto e alla sua vera grandezza[58]. Tale crescente interesse per questo argomento è in parte correlato ai suoi effetti sul comportamento dei consumatori quando questi richiedono prodotti economici di alta qualità alle organizzazioni[59]. L'integrazione di entrambi i concetti è così importante che alcuni autori hanno accennato al ruolo guida che il *marketing* dovrebbe svolgere nell'analisi della RSI[60] e alcuni hanno persino tentato di dare una definizione di tali forme di responsabilità nel campo del *marketing*[61]. È sempre stato ipotizzato che il *marketing* avvenga in un contesto sociale. I concetti chiave del *marketing* come disciplina sociale sono sempre stati collegati agli scambi tra agenti sociali, individui, gruppi e organizzazioni e come proclamato da Hunt, "la scienza del *marketing* è la scienza comportamentale che cerca di spiegare le relazioni di

---

[58] MARÍN L., RUIZ S., RUBIO A. (2009), *The role of identity salience in the effects of corporate social responsibility on consumer behavior*, Journal of Business Ethics, 84, 65-78.

[59] SEN S., BHATTACHARYA C. B. (2001), *Does doing good always lead to doing better? consumer reactions to corporate social responsibility*, Journal of Marketing Research, XXXVIII, 225-243.

[60] LANTOS G. (2001), *The boundaries of strategic corporate social responsibility*, The Journal of Consumer Marketing, 18(7), 595-630.

[61] VAALAND T., HEIDE M., GRONHAUG K. (2008), *Corporate social responsibility: Investigating theory and research in the marketing context*, European Journal of Marketing, 42(9/10), 927-953.

scambio"[62]. Questa definizione è stata riformulata nel tempo, fino ad arrivare all'ultima definizione proposta dall'*American Marketing Association* (AMA) nel 2017 secondo cui "il *marketing* è l'attività, l'insieme di istituzioni e processi per la creazione, la comunicazione, la consegna e lo scambio di offerte che hanno valore per clienti, clienti, *partner* e società in generale"[63]. La definizione dell'AMA riguarda i ruoli e le responsabilità del *marketing* in relazione alla società: afferma che il *marketing* costruisce, consegna e dovrebbe offrire un valore globale non solo ai clienti e ai consumatori e a un'azienda, ma anche alla società nel suo insieme. Allo stesso modo, la definizione di *marketing* a un livello più globale sembra evidenziare l'esistenza e il contributo di molte attività di *marketing*, istituzioni e processi oltre a quelli di una singola azienda e dei suoi dirigenti, che è stato tradizionalmente il suo campo di azione. D'altra parte, l'attuale definizione, che considera gli aspetti aggiunti dal *marketing*, estende il rapporto tra *marketing* e altre discipline come il *management*, in cui gli aspetti principali della RSI sono stati discussi in modo estensivo. Infine, questa definizione, attraverso le proprietà sistemiche a cui si rivolge tacitamente, viene facilmente tradotta in concettualizzazioni dei mercati e influenzata dalle azioni delle aziende e della disciplina, implicando così stretti legami tra le organizzazioni e le società in cui operano. È stato dimostrato che ci sono stati notevoli analisi sulla RSI nell'ambito della disciplina del *marketing*,

---

[62] HUNT S. D. (1983), *General theories and the fundamental explananda of marketing*, Journal of Marketing, 47(4), 9-17, p. 13.

[63] AMERICAN MARKETING ASSOCIATION (AMA) è la comunità essenziale per gli esperti di *marketing*. Oggi l'AMA conduce una discussione senza pari sull'eccellenza del *marketing*. L'ultima definizione, approvata nel 2017, è disponibile *online* al seguente indirizzo *world wide web*: https://www.ama.org/the-definition-of-marketing-what-is-marketing/. Data di ultimo accesso e consultazione: 19 febbraio 2020.

e le principali prospettive includono: *cause-related marketing*, il *marketing* ambientale[64], le risposte dei consumatori alle azioni di RSI delle imprese, il *marketing* sociale, con *focus* sulla qualità della vita, acquisti socialmente responsabili e consumo sostenibile[65]. Le cinque principali prospettive teoriche dei due costrutti[66] presenti in letteratura sono le seguenti: 1. Ampliamento del concetto di *marketing*: l'applicazione dei principali concetti e tecniche di *marketing* per il supporto degli obiettivi e dei ruoli sociali delle imprese. Il *marketing* deve essere applicato per scopi che vanno oltre la mera promozione dei beni di consumo; 2. *Marketing* e società: *marketing* e sviluppo economico, *macromarketing*, contributi di *marketing* alla società nel suo insieme e opportunità commerciali al "fondo della piramide". Il sistema di *marketing* è analizzato nella sua interezza; 3. Dimensioni specifiche della responsabilità sociale nel *marketing*: etica del *marketing*; vendita al dettaglio e RSI; *social marketing*; *cause-related marketing*; commercio equo, consumo responsabile e vulnerabilità dei consumatori; filantropia; *marketing* verde e *greenwashing* e *marketing* responsabile. Gli aspetti sociali / ambientali sono collegati agli aspetti economici e sono collegati al *marketing* integrando l'applicabilità e un ambito specifico ai costrutti della RSI in questa disciplina; 4. RSI, associazioni aziendali, immagini,

---

[64] Sul *marketing* ambientale si veda BAI X., CHANG J. (2015), *Corporate social responsibility and firm performance: The mediating role of marketing competence and the moderating role of market environment*, Asia Pacific Journal of Management, 32, 505-530.

[65] DOLAN P. (2002), *The sustainability of "sustainable consumption"*, Journal of Macromarketing, 22(2), 170-181.

[66] SANCLEMENTE J. C. (2012), *Marketing y la RSE. Lo social como estrategia de marketing*, in RAUFFLET E., LOZANO J. F., BARRERA E., GARCIA C. (Eds.), *Responsabilidad Social Empresarial*, pp. 145-156, México: Pearson Educación.

reputazione e *stakeholder*: quest'area esamina le azioni RSI come strumento di comunicazione per aumentare la fedeltà dei consumatori e per costruire reputazione, *marketing* aziendale, identificazione dei consumatori e risposte (associazioni percettive) alle società in base alle loro azioni di RSI. Vengono inoltre prese in considerazione le esigenze degli *stakeholder*; 5. La relazione tra RSI e prestazioni complessive dell'azienda: ciò implica di considerare la RSI come una strategia aziendale e come una fonte di vantaggio competitivo nelle organizzazioni. Le prestazioni di una società sono anche associate alle azioni intraprese al riguardo[67]. Un *marketing management* efficace e di successo nel lungo periodo deve essere accompagnato da un forte senso di responsabilità sociale e dall'adozione di valori e principi etici quali guida di piani e azioni. Varie forze spingono le imprese a impegnarsi maggiormente in questo senso: le crescenti aspettative del cliente, la sensibilità diffusa nella società, gli obiettivi e le ambizioni del personale aziendale, le normative e la crescente pressione da parte degli enti governativi, l'interesse degli investitori per l'uso di criteri di responsabilità sociale (la cosiddetta finanza etica), l'attenzione da parte dei media e i mutamenti nelle pratiche di acquisizione delle risorse[68]. Le imprese non hanno sempre creduto nel valore della responsabilità sociale. Nel 1776 Adam Smith dichiarò: "non ho mai notato il bene fatto da coloro che professano

[67] BHATTACHARYA C. B., SMITH N. C., VOGEL D. (2004), *Integrating social responsibility and marketing strategy: An introduction*, California Management Review, 47(1), 5-8.

[68] Cfr. *Special Report: Corporate Social Responsibility*, The Economist, 17 gennaio 2018. Per una prospettiva accademica più ampia si rimanda a PORTER M. E., KRAMER M. R. (2006), *Strategy & Society*, Harvard Business Review, 78-92; CHRISTENSEN C. M., BAUMANN H., RUGGLES R., STADTLER T. M. (2006), *Disruption Innovation for Social Change*, Harvard Business Review, 94-101.

di praticare il commercio in nome del bene comune"[69]. Secondo il padre fondatore della moderna economia politica, qualunque azione che si propone come scopo diretto quello di promuovere il bene comune produce effetti perversi per l'impresa e per la società. All'opposto, qualora si agisca in vista del proprio interesse, la nota mano invisibile può guidare i diversi agenti a conseguire uno scopo che non era nelle intenzioni originarie, ovvero il benessere di tutta la società. La posizione della teoria neoclassica dell'impresa sulla RSI è sintetizzata con la storica frase del leggendario economista della scuola di Chicago e premio *Nobel* per l'Economia nel 1976, Milton Friedman, il quale definì le iniziative sociali "fondamentalmente sovversive", ritenendo che minassero lo scopo di lucro delle imprese, sprecando il denaro degli azionisti[70]. Friedman, considerato l'esponente più rappresentativo dei critici della RSI, intesa in senso non strumentale/normativo, fa riferimento a un contesto di regole del gioco[71] che in qualche modo orientano il perseguimento del profitto da parte dell'impresa. Alcuni autori temono addirittura che gli investimenti in aree importanti come la ricerca e l'innovazione possano risentire dello spostamento dell'attenzione sulla

[69] SMITH A. (1776), *An Inquiry into the Nature and Causes of the Wealth of Nations*, p. 456.

[70] FRIEDMAN M. (1962), *Capitalism and Freedom*, University of Chicago Press. Secondo l'autore, p. 133 ss., «C'è una e una sola responsabilità sociale dell'impresa, usare le sue risorse e dedicarsi ad attività volte ad incrementare i propri profitti a patto che essa rimanga all'interno delle regole del gioco il che equivale a sostenere che compete apertamente senza ricorrere all'inganno o alla frode».

[71] VERDE M. (2017), *Responsabilità sociale di impresa tra teoria e prassi. Il bilancio sociale come processo di costruzione di senso*, G. Giappichelli Editore, Torino, p. 13.

responsabilità sociale[72]. I critici costituiscono però una sparuta minoranza. Per accrescere il livello di responsabilità sociale delle attività di *marketing*, l'impresa deve agire puntando a un comportamento legale, etico e socialmente responsabile[73]. Le imprese devono assicurarsi che tutti i loro dipendenti conoscano e osservino le leggi che li riguardano. In aggiunta, le attività di impresa possono diventare oggetto di critica perché vi sono situazioni che pongono sistematicamente dei dilemmi etici. Non è semplice tracciare una distinzione netta tra una normale pratica di *marketing* e un comportamento eticamente scorretto. In quest'ottica, le imprese dovrebbero adottare e diffondere un codice etico scritto, fare del comportamento etico un principio basilare e responsabilizzare pienamente il personale rispetto alle direttive di carattere etico e legale. Le imprese devono applicare la loro "coscienza sociale" ai rapporti con i clienti e con i diversi soggetti coinvolti nell'attività. Sempre più spesso i consumatori desiderano informarsi sull'impegno sociale delle imprese, per scegliere quelle in cui essere

---

[72] GROW B., *The Debate over Doing Good*, BusinessWeek, 15 agosto 2005.

[73] KOTLER P., KELLER K. L., ANCARANI F., COSTABILE M. (2017), *Marketing Management*, Pearson Italia, quindicesima edizione traduzione italiana, Milano, p. 136 ss. Edizione originale: KOTLER P. (1967), *Marketing Management: Analysis, Planning, and Control*, Prentice Hall, Englewood Cliffs, NY. È il manuale di *marketing* di gran lunga più longevo e noto del mondo. Philip Kotler, nato a Chicago il 17 maggio del 1931, è considerato uno dei massimi esperti mondiali nell'ambito del *marketing management*. L'attualità del suo pensiero fa di Kotler una personalità ancora oggi di spicco e intensamente impegnata in conferenze presso università, enti ed aziende a livello internazionale. Kotler rappresenta una figura indiscutibilmente rilevante nel panorama mondiale del *management*, tanto che il *Financial Times* l'ha definito uno dei quattro *guru* del *management* di tutti i tempi assieme a Jack Welch, Bill Gates e Peter Drucker.

clienti, su cui investire e in cui lavorare. Per questo motivo le imprese comunicano la difficile sfida della responsabilità sociale nel proprio bilancio sociale, un documento che testimonia l'impegno dell'impresa al perseguimento di obiettivi socialmente responsabili[74]. Talvolta anche le iniziative filantropiche possono rivelarsi problematiche. Le iniziative meritevoli corrono il rischio di essere sottovalutate, o addirittura disapprovate, se l'impresa appare animata solamente dalla volontà di ricavarne un profitto e non riesce a sviluppare un'immagine credibile e positiva. Le imprese che sapranno individuare soluzioni e valori innovativi mantenendo comportamenti socialmente responsabili avranno maggiori probabilità di successo. La responsabilità sociale, declinata nelle forme del *marketing* legato a cause benefiche e dei programmi di volontariato per il personale, è ritenuta dalle imprese giusta e intelligente. Nel *cause-related marketing* i contributi che un'impresa versa a favore di una determinata causa benefica sono legati alla partecipazione diretta o indiretta dei clienti a transazioni che generino profitto per l'impresa stessa. Un programma di questo tipo può migliorare il benessere collettivo, contribuire alla differenziazione e al posizionamento della marca, creare legami solidi con i consumatori, migliorare l'immagine pubblica dell'impresa, alimentare gli atteggiamenti positivi verso le sue marche, motivare e stimolare il personale e incrementare le vendite e accrescere così il valore di mercato dell'impresa. I consumatori possono dunque sviluppare nei confronti dell'impresa un legame forte ed esclusivo, che non si limiti alle sole transazioni commerciali. Più specificatamente, il *marketing* delle

[74] Per approfondimenti legati al bilancio sociale si rimanda a RUSCONI G. (2013), *Il bilancio sociale delle imprese: economia, etica e responsabilità sociale dell'impresa*, Ediesse, Roma.

cause sociali[75] è in grado di: 1. diffondere la conoscenza della marca; 2. migliorare l'immagine della marca; 3. conferire alla marca maggiore credibilità; 4. evocare sentimenti positivi nei confronti della marca; 5. creare un senso di comunità attorno alla marca; 6. creare legami affettivi tra la marca e i consumatori. Questo tipo di *marketing* può essere controproducente qualora i consumatori mettano in discussione la relazione tra il prodotto e la causa adottata o percepiscano che l'impresa intende in realtà sfruttare la causa per interessi propri. I problemi possono sorgere anche quando i consumatori ritengono che l'impresa non sia coerente né sufficientemente responsabile in tutti i suoi comportamenti. In un periodo di crisi economica, tra tutte le funzioni aziendali il *marketing* è forse quella che più spesso viene messa sul banco degli imputati. Alla disciplina e alle sue diverse applicazioni viene generalmente attribuita la colpa di avere promosso

[75] La letteratura inerente al *cause-related marketing* è sterminata: SIMCIC P., BELLIU A. (2001), *Corporate social responsibility and cause-related marketing: An overview*, International Journal of Advertising, 20, 207-222; BLOOM P. N., HOEFFLER S., KELLER K. L., BASURTO C. E. (2006), *How Social-Cause Marketing Affects Consumer Perceptions*, MIT Sloan Management Review 47(2), 49-55; SIMMONS C. J., BECKER-OLSEN K. L. (2006), *Achieving Marketing Objectives through Social Sponsorships*, Journal of Marketing, 70(4), 154-169; BERENS G., VAN RIEL C. B. M., VAN BRUGGEN G. H. (2005), *Corporate Associations and Consumer Product Responses: The Moderating Role of Corporate Brand Dominance*, Journal of Marketing, 69(3), 35-48; LICHTENSTEIN D. R., DRUMWRIGHT M. E., BRAIG B. M. (2004), *The Effect of Corporate Social Responsibility on Customer Donations to Corporate-Supported Nonprofits*, Journal of Marketing, 68(4), 16-32; HOEFFLER S., KELLER K. L. (2002), *Building Brand Equity through Corporate Societal Marketing*, Journal of Public Policy & Marketing, 21(1), 78-89; VARADARAJAN P., MENON A. (1988), *Cause-related marketing: To coalignment of marketing strategy and corporate philanthropy*, Journal of Marketing, 52, 58-74.

l'iperconsumismo e le sue conseguenze sociali. Il *marketing* classico nella sua formulazione originaria ha come unico obiettivo quello di garantire la soddisfazione del singolo consumatore nel momento stesso del consumo, mentre invece mediante il *marketing* responsabile l'impresa – seguendo l'ottica della *customer advocacy* – si prende carico del benessere complessivo del cliente, anche a costo di ridurne il consumo o indirizzarlo indirettamente verso offerte concorrenti. In questo contesto esiste un vincolo in più: garantire la soddisfazione del cliente anche nel caso di acquisto e consumo prolungati nel tempo[76]. La vera sfida del nuovo *marketing* è abbracciare l'area della sostenibilità[77]: in questo caso il beneficio di breve e lungo periodo della collettività si affianca e non si sostituisce al vantaggio del consumatore, per garantire la sostenibilità economica oltre che ambientale e sociale dell'impresa. L'impresa che voglia avviarsi verso un percorso di sostenibilità deve sostanzialmente ampliare lo spettro delle proprie responsabilità. Un approccio sostenibile[78], ossia

[76] PRATESI C. A. (2013), *Verso il marketing sostenibile*, in MATTIACCI A., PASTORE A. (a cura di), *Marketing. Il management orientato al mercato*, Hoepli, Milano, pp. 586-599. Secondo l'autore, p. 591, *per customer advocacy* si intende "l'attività che viene svolta dalle imprese per tutelare gli interessi dei loro clienti, aiutandoli a raggiungere un obiettivo in termini di benessere di lungo periodo anche al di là delle loro esplicite richieste e, quindi, di quella che generalmente viene considerata la *customer satisfaction*".

[77] Sempre secondo PRATESI C. A. (2013), op. cit., p. 594, la traduzione letterale di *sustainability* in "sostenibilità" può generare confusione. Infatti, in italiano, almeno nel linguaggio comune, sostenibile viene inteso come sinonimo di "tollerabile" o "sopportabile". La traduzione corretta sarebbe "durevole", proprio come propongono i francesi traducendo "sviluppo sostenibile" con il termine *développement durable*.

[78] Sul tema della sostenibilità cfr. GIACOMETTI A. (2013), *Il marketing sostenibile: dal dire al fare business, responsabilmente. Principi, metodi*

capace di far sopravvivere l'impresa nel lungo periodo, impone ben altre attenzioni che il mero perseguimento della creazione di valore per gli azionisti[79]. Nel tempo si è chiesto alle imprese di tenere in considerazione degli interessi dei lavoratori e della *customer satisfaction*. Per poter rispondere a queste nuove e complesse sfide, le imprese non possono limitarsi ad agire da sole, ma devono farsi carico di tutta la filiera all'interno della quale operano: sia a valle, verso il *trade* e i consumatori, sia a monte verso i fornitori. In altri termini, in passato fu proprio il *marketing* a mettere in risalto la centralità del cliente, mentre oggi lo stesso impegno deve essere profuso verso tutti gli *stakeholder* (dimensione verticale), lungo tutta la filiera (dimensione orizzontale), e mantenuto costante nel tempo. E soprattutto le imprese sono chiamate ad adottare una prospettiva di lungo periodo, molto distante dal consueto approccio, estremizzato negli ultimi anni dal mondo della finanza, ma gradito anche dagli economisti, a partire da Keynes che coniò il celebre aforisma: «*In the long run we are all dead*»[80]. Facile quindi prevedere che

---

*e strumenti per innovare col Marketing la Responsabilità Sociale d'Impresa (CSR) in chiave sostenibile ed etica*, Maggioli Editore, Santarcangelo di Romagna; per un quadro critico cfr. DE GIROLAMO S., D'ANSELMI P. (2017), *La responsabilità sociale delle organizzazioni. L'impresa sostenibile e lo sviluppo competitivo*, FrancoAngeli, Milano; con particolare riferimento agli aspetti di *governance*, comunicazione, *accountability* cfr. BALLUCHI F., FURLOTTI K. (a cura di) (2017), *La responsabilità sociale delle imprese. Un percorso verso lo sviluppo sostenibile. Profili di governance e di accountability*, G. Giappichelli Editore, Torino.

[79] Per una interessante *review* sistematica della letteratura sul punto cfr. PELOZA J., SHANG J. (2011), *How can corporate social responsibility activities create value for stakeholders? A systematic review*, Journal of the Academic Marketing Science, 39, 117-135.

[80] Trad. it. "Nel lungo periodo siamo tutti morti", JOHN MAYNARD KEYNES (1883-1946), il grande economista britannico, scrisse il celebre

chi si ostinerà a mantenere un atteggiamento di breve periodo, ancorato a un vecchio modo di pensare al valore dell'impresa, più vicino alle questioni finanziarie che a quelle sociali, rischierà grosso, perché un qualunque minimo sussulto dell'opinione pubblica potrà avere effetti catastrofici sui suoi risultati economici. Il *marketing* responsabile richiede la comprensione dei ritorni, finanziari e non, dei programmi di *marketing* in una prospettiva ampia. Oltre ai ricavi di vendita si valuta cosa accade alla quota di mercato, al tasso di abbandono dei clienti, alla loro soddisfazione e ad altre misure che possono giungere a considerare gli effetti legali, etici, sociali e ambientali delle attività di *marketing* dell'impresa.

### *4.2 La misurazione della performance*

La misurazione della *performance* di *marketing* in logica olistica viene estesa sino a includere la prospettiva dei principali *stakeholder* accrescendo in questo modo la responsabilità dei *marketing manager* sia verso l'impresa che verso l'ambiente esterno. Un'ampia varietà di indici finanziari viene utilizzata per determinare il valore diretto e indiretto creato dall'attività di *marketing* e si riconosce che gran parte del valore di mercato dell'impresa deriva da *asset* intangibili, in particolare marchi, base-clienti, personale, relazioni con distributori e fornitori, capitale intellettuale. Le metriche di *marketing* possono aiutare le imprese a quantificare e confrontare le *performance* di *marketing* lungo numerose dimensioni e servono a guidare i comportamenti responsabili del personale aziendale nella creazione di valore e a controllare e reindirizzare i

aforisma nel dicembre 1923 in *A Tract on Monetary Reform*, ch. 3, p. 80, sul dibattito in Gran Bretagna sul ripristino del sistema di cambio fisso pre-Prima Guerra Mondiale noto come *Gold Standard*.

comportamenti dell'impresa. Il *marketing* socialmente responsabile è dunque visto come un'estensione del concetto di *Corporate Social Responsibility* (CSR). È fondamentale capire se e in quale misura le azioni di responsabilità sociale hanno un impatto diretto sui risultati economico finanziari dell'impresa al fine di dare legittimazione all'investimento di risorse in tali attività[81]. Per tale ragione è stato introdotto il concetto di *Performance* Sociale d'Impresa o *Corporate Social Performance* (CSP) facendo riferimento ad un modello d'analisi composto da molteplici dimensioni interconnesse, 1. la *corporate social responsibility* ($CSR_1$), che consiste nella definizione delle responsabilità che l'impresa ha nei confronti della società in cui opera; 2. la *corporate social responsiveness* ($CSR_2$), che comprende la rispondenza verso i problemi sociali; 3. le *social issues*, ossia l'identificazione delle problematiche e delle aree di interesse cui rivolgersi[82]. L'approccio della *Corporate Social Performance* è stato introdotto nel 1979 da Carroll come strumento di risposta dell'impresa ai problemi sociali, con specifico riferimento al contesto nel quale le politiche di RSI avranno effetto nella strategia d'impresa[83].

---

[81] USEEM M. (1996), *Investor Capitalism: How Money Managers are Changing the Face of Corporate America*, New York, Basic Books.

[82] Cfr. BARNETT M. L. (2007), *Stakeholder influence capacity and the variability of financial returns to corporate social responsibility*, Academy of Management Review, 32; FREDERICK W. C. (2006), *Corporation, Be Good! The Story of Corporate Social Responsibility*, Indianapolis, IN, Dog Ear Publishing; MCWILLIAMS A., SIEGEL D., WRIGHT P. M. (2006), *Corporate social responsibility: Strategic Implications*, Journal of Management Studies, 43; WOOD D. J. (1991), *Corporate social performance revisited*, Academy of Management Review, 16; WOOD D. J. (1991), *Social issues in management: Theory and research in corporate social performance*, Journal of Management, 17, 383–406.

[83] CARROLL A. B. (1979), *A three-dimensional conceptual model of corporate performance*, Academy of Management Review, 4(4), 479-

La *performance* sociale d'impresa viene utilizzata come *proxy* dell'efficacia dei sistemi di responsabilità sociale implementati al fine di misurare la capacità aziendale di sviluppare e gestire tali politiche e può essere vista come la risultante dell'interazione di tre dimensioni[84]: 1. le singole dimensioni che compongono la Responsabilità Sociale d'Impresa - economica, legale, etica e discrezionale ($CSR_1$). In questa sede si fa dunque riferimento ad un costrutto che ricomprende le aspettative economiche, legali, etiche discrezionali che la società ha nei confronti dell'organizzazione in un certo orizzonte temporale; 2. la capacità di risposta dell'impresa intesa come il comportamento strategico che l'impresa assume rispetto agli obiettivi sociali prefissati ($CSR_2$); 3. la capacità aziendale di rispondere alle aspettative della società e di gestire le problematiche sociali, intese nel senso più ampio del termine (le *social issues*). Rispetto alla sua responsabilità sociale, un'impresa può assumere diversi atteggiamenti che determinano la sua capacità di risposta e, dunque, il suo livello di *performance* sociale: 1. reattivo; 2. difensivo; 3. accomodativo; e 4. proattivo. L'atteggiamento reattivo parte dalla negazione dell'impresa come soggetto portatore di responsabilità nei confronti della società, che comporta un impegno dell'impresa minore a quanto effettivamente necessario. Si assume una strategia di difesa quando l'impresa pur riconoscendo un certo grado di impegno sociale, di fatto vi si oppone limitandosi a fare lo stretto necessario. L'atteggiamento di tipo accomodativo si concretizza nell'accettare pienamente la responsabilità e ad

505; ID. (1999), *Corporate social responsibility: Evolution of a definitional construct*, Business & Society 38(3), 268-295, p. 287.

[84] CARROLL A. B. (1979), op. cit.; WARTICK S., COCHRAN P. (1985), *The evolution of the corporate social performance model*, Academy of Management Review, 10; WOOD D. J. (1991), op. cit.

implementare tutte le azioni sociali richieste dall'ambiente esterno. Infine, l'impresa si comporta in maniera proattiva quando, anticipando la manifestazione di bisogni sociali, si impegna totalmente in azioni di responsabilità sociale[85]. La letteratura accademica suggerisce molteplici benefici direttamente collegati all'implementazione di politiche di RSI nelle aziende, quali: 1. miglioramento dell'immagine aziendale rispetto a clienti, finanziatori e fornitori[86]; 2. impatto positivo sulla reputazione dell'impresa[87] e sulla *corporate identity*[88]; 3. aiuta l'impresa a ricevere supporto dai propri *stakeholder*, fondamentali per la sua sopravvivenza[89]; 4. contribuisce al raggiungimento di un vantaggio competitivo attraverso una riduzione dei costi di transazione e di agenzia dell'impresa[90]; 5. aumenta il capitale relazionale dell'impresa[91]; 6. aiuta l'impresa a

[85] CLARKSON M. B. E. (1995), *A Stakeholder Framework for Analyzing and Evaluating Corporate Social Performance*, The Academy of Management Review, 20(1), 92-117.

[86] FOMBRUN C., SHANLEY M. (1990), *What's in a name? Reputation building and corporate strategy*, Academy of Management Journal, 33, 233–258.

[87] ZYGLIDOPOULOS S. C. (2002), *The social and environmental responsibilities of multinationals: evidence from the brent spar case*, Journal of Business Ethics, 36 (1-2); MCWILLIAMS A., SIEGEL D. (2001), *Corporate Social Responsibility: a theory of the firm perspective, Academy of Management Review*, 26 (1).

[88] HOSMER L. T. (1994), *Strategic Planning as if Ethics mattered, Strategic Management Journal*, 15.

[89] CLARKSON M. B. E. (1995), *A Stakeholder Framework for Analyzing and Evaluating Corporate Social Performance*, The Academy of Management Review, 20(1), 92-117.

[90] JONES T. M. (1995), *Instrumental stakeholder theory: a synthesis of ethics and economics*, Academy of Management Review, 20(2), 404–437.

[91] BARNEY J. B., HANSEN M. H. (1994), *Trustworthiness as a source of competitive advantage*, Strategic Management Journal, 15; NAHAPIET J., GHOSAL S. (1998), *Social capital, intellectual capital, and the*

reperire migliori risorse umane[92] e a valorizzare quelle presenti in azienda; 7. rappresenta uno strumento di differenziazione del prodotto[93]; 8. rappresenta uno strumento assicurativo capace di tutelare la *performance* finanziaria dell'impresa[94]. Numerosi benefici sono, dunque, riconducibili all'introduzione di condotte socialmente responsabili nelle prassi aziendali, nonostante numerosi quesiti che devono ancora essere investigati in letteratura al fine di dare evidenza empirica di una relazione positiva tra la *performance* sociale dell'impresa e la sua *performance* economico-finanziaria[95]. Altro indicatore della misurazione della *performance* sociale è rappresentato dal Valore Condiviso o *Shared Value* (SV), definito da Porter e Kramer (2011) come l'insieme delle politiche e delle pratiche operative che rafforzano la competitività di un'azienda, migliorando nello stesso tempo le condizioni economiche e sociali delle comunità in cui opera. Una CSR di successo non si limita a tutelare i

---

*organizational advantage*, Academy of management review, 23(2); WADDOCK S. A., GRAVES S. B. (1997), *The corporate social performance-financial performance link*, Strategic Management Journal, 18(4).

[92] GREENING D. W., TURBAN D. B. (2000), *Corporate social performace as a competitive advantage in attracting a quality workforce*, Business and Society, 39, 254-280.

[93] MCWILLIAMS A., SIEGEL D. (2001), *Corporate Social Responsibility: a theory of the firm perspective, Academy of Management Review*, 26 (1).

[94] GODFREY P. C., MERRILL C. B., HANSEN J. M. (2009), *The relationship between corporate social responsibility and shareholder value: an empirical test of the risk management hypothesis*, Strategic Management Journal, 30(4), 425-445.

[95] GANGI F., MUSTILLI M. (2018), *La responsabilità sociale d'impresa. Principi e pratiche*, Egea, Milano, p. 76 ss; CAROLI M. G., TANTALO C. (a cura di) (2010), *La responsabilità sociale d'impresa nel quadro delle "linee guida OCSE destinate alle imprese multinazionali". Un focus sulle piccole e medie imprese*, Rapporto di ricerca con il patrocinio dell'Istituto per la promozione industriale (IPI) e del Ministero dello Sviluppo Economico (MiSE), Roma, Luiss Business School, p. 1-243.

diritti, ma agisce anche per generare lo SV attraverso pratiche che migliorano la competitività dell'azienda e, al tempo stesso, le condizioni economiche e sociali all'interno della società in cui essa opera. Produrre SV vuol dire sviluppare soluzioni mirate a rispondere alle istanze di più classi di interlocutori elaborando progetti aziendali complessi, le «Sintesi Socio Economiche» (SSE). Una SSE produce un vantaggio competitivo attraverso la soddisfazione degli *stakeholder*, conciliando l'interesse dell'azienda al conseguimento del profitto con le esigenze della tutela dell'ambiente e della solidarietà sociale. L'assunto di base è che se le imprese sono in grado di generare effetti moltiplicatori sull'ambiente circostante, anche quest'ultimo incide sul risultato delle imprese. Si devono trovare i punti d'incontro tra la strategia aziendale e le esigenze della società. Questi punti d'incontro non risiedono solo laddove lo sviluppo del *business* può beneficiare a temi ambientali o sociali (definiti *inside-out linkages*), ma anche laddove, viceversa, la società impatta positivamente sulle *performance* dell'impresa (*outside-in linkages*). Un rilievo fondamentale è assunto dall'analisi del tessuto imprenditoriale e associativo circostante per la creazione di sinergie capaci di alimentare la catena del valore. Lo SV non scaturisce da una mera redistribuzione dei profitti aziendali per scopi sociali (*charity principle*), ma dalla capacità di un *business* di collaborare, in itinere, allo sviluppo sociale. Una volta compresi i punti di contatto tra *business* e società, l'impresa dovrà operare una scelta. Porter e Kramer classificano le questioni sociali in tre categorie: a) *Generic social issues* (problemi sociali generici), che per quanto importanti, non scaturiscono o influenzano più di tanto l'operato e la competitività aziendale; b) *Value chain social impacts* (impatti sociali della catena del valore), ovvero gli ambiti sociali in cui l'azienda incide in modo sostanziale; c) *Social dimension*

*of competitive context* (dimensione sociale del contesto competitivo), in cui si tratta di quei fattori esterni che incidono significativamente su *performance* e competitività dell'azienda. Sempre secondo Porter e Kramer, gli approcci possibili per creare valore condiviso sono tre: 1) riconcepire prodotti e mercati; 2) ridefinire la produttività nella catena del valore; e 3) facilitare lo sviluppo di *cluster* locali (agglomerati di imprese, fornitori, università, associazioni, *asset* pubblici) con cui l'impresa, in un territorio, si relaziona anche indirettamente In ogni caso, si attraversa il c.d. circolo virtuoso del valore condiviso, per cui la creazione di valore in un'area - economica, sociale, o ambientale - si ripercuote positivamente anche sulle altre due, dando vita all'opportunità di soddisfare nuovi bisogni, aumentare l'efficienza, differenziare, espandere i mercati[96].

## 5. Funzione sociale ed etica nel governo d'impresa

Nel governo dell'impresa, e soprattutto nell'attuazione del processo decisorio, il ruolo centrale è quello dei valori, ovvero dei criteri in base ai quali chi opera in un'organizzazione assume le decisioni di gestione. L'etica è definita come la scienza della condotta, in quanto detta le regole morali da seguire nell'assunzione delle scelte e dei comportamenti. Le virtù etiche sono il coraggio, la temperanza, la liberalità, la magnanimità, la franchezza e, soprattutto, la giustizia[97]. L'etica rappresenta un importante criterio di guida nelle decisioni e nei comportamenti individuali aziendali, proteso al rispetto di

[96] Cfr. PORTER M. E., KRAMER M. R. (2011), *The Big Idea: Creating Shared Value. How to Reinvent Capitalism—and Unleash a Wave of Innovation and Growth*, Harvard Business Review, 89(1-2), 62-77.

[97] ABBAGNANO N. (1961), *Dizionario di filosofia*, UTET, Torino.

valori morali fondamentali. L'etica applicata al mondo degli affari e in particolare all'impresa non può rifarsi alle teorie etiche generali ma deve essere oggetto di opportuni adattamenti in funzione delle peculiarità della gestione aziendale[98]. Questi andamenti si giustificano sulla base di tre motivi[99]: 1. la necessità di ritrovare in ogni scelta un corretto equilibrio tra obiettivi economici e sociali; 2. la pluralità e multiformità di aspetti da considerare e valutare in ciascun problema aziendale; 3. il naturale collegamento tra le decisioni da assumere. Dunque, l'etica aziendale, poiché è rivolta a conciliare gli obiettivi economici e le responsabilità sociali, può essere considerata in definitiva come un modello comportamentale di sintesi funzionale allo sviluppo dell'impresa e alle finalità dell'imprenditore nel lungo termine. All'interno dell'etica aziendale[100] si distinguono gli aspetti relativi: (a) all'etica dell'impresa, (b) all'etica nell'impresa e (c) all'etica manageriale. L'introduzione di valori etici nel processo decisionale

[98] Degno di particolare nota è il fatto che in merito alla etica d'impresa (*business ethics*) si pubblicano ormai da tempo quattro riviste di rilevanza internazionale: a) *Journal of Business Ethics*; b) *Business Ethics Quarterly*; c) *Business Ethics, a European Review*; d) *Business and Professional Ethics Journal*.

[99] Il *Josephson Institute of Ethics* ha individuato dodici princìpi che la maggior parte degli individui associa al comportamento etico e che dovrebbero essere sistematicamente considerati per assumere decisioni etiche: onestà, probità, lealtà, equità, affidabilità, assistenza agli altri, rispetto per gli altri, ossequio per le leggi, motivazione all'eccellenza, *leadership*, reputazione e responsabilità personale.

[100] L'opportunità di distinguere tra etica manageriale (livello individuale), etica aziendale (livello micro-sistemico) ed etica economica (che raggruppa la *corporate ethics* e l'etica economica dei gruppi sociali) sottolinea la difficile traducibilità della *business ethics*, che viene resa intercambiabilmente come "etica d'impresa", "etica aziendale" o "etica degli affari".

dell'impresa passa attraverso tre stadi[101]: 1. l'individuazione di un dilemma etico; 2. la selezione di uno *standard* etico di riferimento; 3. l'applicazione dello *standard* etico nella scelta. La questione di fondo s'incentra sull'ampia discrezionalità teoricamente attribuita al *manager* di identificare e nel voler risolvere un problema con connotazioni etiche oltre che economiche[102]. L'impatto dei gradi di libertà esercitabili sul progresso dell'etica nell'impresa è variabile, dato che il *manager* può avere una discrezionalità limitata o piena, oppure non averla. Un avanzamento sostanziale si verifica quando l'etica viene considerata come un'opportunità e non come un vincolo nel governo d'impresa. In quest'ottica si passa dal concetto di rispetto dei valori etici per poter raggiungere le finalità economico-aziendali, a quello di adozione dell'etica quale leva per lo sviluppo nel medio-lungo termine. La credibilità o affidabilità sociale diviene così un valore strategico, spendibile nei rapporti competitivi e nelle alleanze interaziendali[103]. In altri termini, i princìpi etici non devono

---

[101] MURPHY P. E., LACZNIAK G. R., BOWIE N. E., KLEIN T. A. (2005), *Ethical Marketing*, Pearson, Upper Saddle River, NJ. Il volume esplora le questioni etiche che devono affrontare i professionisti del *marketing* e presenta la teoria etica nel contesto del *marketing*.

[102] HOSMER L. T. (1991), *The Ethics of Management*, Irwin, Homewood, IL. L'autore, op. cit., osserva che per pervenire a una decisione che sia eticamente giusta, corretta e appropriata, occorre applicare concetti economici, precetti giuridici e princìpi filosofici e che nell'attuazione del processo decisionale, spesso bisogna resistere a forti pressioni organizzative.

[103] In definitiva, l'introduzione dell'etica nell'impresa è conciliabile, soprattutto nell'ottica del lungo termine, con i princìpi economici dell'efficacia e dell'efficienza. L'etica deve essere considerata un'opportunità per migliorare le prospettive di sviluppo dell'impresa e la sua applicazione non può che essere affidata al senso morale di chi dirige l'impresa. Il tema dell'etica si collega a quello della responsabilità sociale d'impresa, declinabile in vari modi ma conseguente in pratica

essere considerati contrapposti ai princìpi economici di efficienza ed efficacia, ma come un sistema complesso di valori capace di conciliare, in modo più equo e durevole, interessi interni ed esterni all'impresa e che consentano lo sviluppo di una gestione aziendale più corretta e il miglioramento dei risultati d'impresa. All'impresa oggigiorno si richiede molto di più rispetto alla tradizionale funzione di produzione, che costituisce comunque l'elemento costitutivo del suo essere ed operare[104]. Difatti, all'impresa viene sempre più insistentemente richiesto di perseguire finalità economiche socialmente qualificate. La funzione sociale deve pertanto accompagnarsi a quella economica ed essere concepita come una precondizione che porta all'esistenza dell'impresa stessa e, al medesimo tempo, come l'attributo che ne assicura la continuità. Il rispetto della responsabilità sociale d'impresa e l'inserimento di criteri etici nelle decisioni aziendali, oltre a garantire buone relazioni con gli *stakeholder* secondari, rispondono ai crescenti attributi di fidelizzazione che

alla presa di coscienza, da parte dell'imprenditore, di dovere rispondere a finalità sociali insieme con quelle economiche e legislative. Il concetto di fondo è che l'impresa non può essere considerata un'organizzazione esclusivamente economica perché rappresenta una cellula della società e in quanto tale è tenuta a perseguire anche altre finalità.

[104] Secondo WERTHER W. B., CHANDLER D. (2010), *Strategic corporate social responsibility*, Sage Publications, Thousand Oaks, pp. 19-20, le quattro tendenze che hanno accresciuto l'importanza della responsabilità sociale d'impresa sono: 1. il crescente benessere, che consente di pagare di più i prodotti; 2. il mutamento delle attese verso le imprese, dovuto anche alla perdita di fiducia nel controllo governativo; 3. la globalizzazione e l'influenza planetaria delle informazioni, che rendono di pubblico dominio in tutto il mondo le cose buone e quelle non buone addebitabili alle imprese; 4. l'attenzione verso la sostenibilità ambientale, acuitasi dappertutto.

l'impresa sviluppa negli *stakeholder* primari[105]. Appare chiara, pertanto, la netta distinzione tra i contenuti della responsabilità sociale e il ruolo dell'etica nell'impresa[106]. La responsabilità sociale fa riferimento al comportamento aziendale nei confronti delle varie collettività di riferimento, mentre l'etica ha un fondamento prevalentemente individuale perché è sempre frutto, nell'impresa, dei valori dei singoli individui formanti la struttura organizzativa[107]. L'impresa si configura come un'istituzione sociale[108] poiché produce effetti (sia positivi

[105] WERTHER W. B., CHANDLER D. (2010), *Strategic corporate social responsibility: Stakeholders in a global environment*, Sage Publications, Thousand Oaks.

[106] SCIARELLLI S., SCIARELLI M. (2018), *Il governo etico d'impresa*, Cedam, Padova, in particolare parte terza intitolata "La responsabilità sociale e l'etica nell'impresa", p. 133 ss. Secondo l'attenta riflessione degli autori, op. cit., l'etica nell'impresa assume caratteristiche del tutto peculiari perché non può essere certo assoluta, va attuata in modo pragmatico e deriva dal comportamento dei soggetti che costituiscono l'organizzazione. In altri termini, l'etica aziendale è dunque un'etica relativa, derivata e pragmatica. Un punto fondamentale nell'impostazione concettuale di questo tema è rappresentato dalla distinzione tra legge, morale ed etica, che sancisce la differenza tra obblighi da rispettare, valori da condividere e coscienza individuale da applicare nei casi concreti. È quest'ultima che consente, infatti, di risolvere i dilemmi etici e che, in ultima analisi, rappresenta (o dovrebbe rappresentare) il filtro finale di scelte aziendali eticamente connotate.

[107] Un'ipotesi di inclusione dei valori etici nel concetto di responsabilità sociale fu avanzata da FREDERICK W. C. (1986), op. cit., il quale suggerì di affiancare, alla $CSR_1$ (*corporate social responsibility*) e alla $CSR_2$ (*corporate social responsiveness*), la $CSR_3$ (*corporate social rectitude*).

[108] BUCHHOLZ R. A. (1991), *Corporate responsibility and the good society: From economics to ecology*, Business Horizons, 34(4), 19-31. Nell'ampliamento delle responsabilità aziendali al campo sociale l'impresa fa riferimento a cinque elementi fondamentali: 1. l'impresa ha delle responsabilità che vanno al di là della produzione di beni o

che negativi) che interessano la collettività e che a causa del mutamento del contesto esterno si vanno sempre più ampliando. L'ampliamento del concetto di responsabilità sociale è in linea con l'evoluzione della società, da tempo più attenta e sensibile al comportamento dell'impresa e ai suoi riflessi sulla vita della comunità. Si tratta di un adattamento al mutare del contesto, all'interno del quale si è venuto a disegnare un ruolo più socialmente qualificato per l'attività d'impresa[109]. L'applicazione dell'etica alle decisioni di *marketing* rappresenta un'esigenza per le imprese, non soltanto per una motivazione reputazionale, ma per rispondere al principio di soddisfazione degli *stakeholder* e, in particolare, dei clienti, in considerazione della differente posizione di forza che le imprese, soprattutto quelle di grandi dimensioni, possono esercitare nei loro confronti[110].

---

servizi con finalità di lucro; 2. le responsabilità si sostanziano nell'aiuto a risolvere importanti problemi sociali, con particolare riferimento a quelli che l'impresa ha contribuito a creare; 3. le imprese devono rendere conto a un pubblico più ampio rispetto ai soli azionisti; 4. le imprese producono effetti che vanno al di là delle semplici transazioni di mercato; 5. le imprese rispondono a un più ampio campo di valori umani rispetto a quelli che possono essere ricompresi nel *focus* esclusivo dei valori economici.

[109] MOLTENI M. (2004), *Responsabilità sociale e performance d'impresa*, Vita e Pensiero - Pubblicazioni dell'Università Cattolica del Sacro Cuore, Milano, p. 103 ss. individua nelle sintesi socio-competitive i comportamenti imprenditoriali tesi a combinare gli aspetti dell'economicità e della socialità della gestione d'impresa. Le sintesi traggono alimento da una cultura tesa al rinnovamento della società, attenta alle attese di tutti gli *stakeholders*, ispirata al coinvolgimento di tutti i collaboratori nello sviluppo dell'impresa.

[110] In merito al tema della applicazione dell'etica nelle decisioni di *marketing* e più in generale dell'evoluzione in senso etico del *marketing* cfr. due importanti volumi monografici: MURPHY P. E., LACZNIAK G. R., BOWIE N. E., KLEIN T. A. (2005), *Ethical Marketing*, Pearson, Upper Saddle River, NJ, passim; vd. SMITH N. C., QUELCH J. A. (1996), *Ethics in*

*Marketing*, McGraw-Hill, New York, passim. I volumi esplorano le questioni etiche che devono affrontare i professionisti del *marketing* e presentano la teoria etica nel contesto del *marketing*. La copertura include pubblicità, sicurezza dei prodotti e mercati mirati, nonché ricerche di mercato, contraffazione dei prodotti, canali di distribuzione, pratiche di vendita e come implementare l'etica nelle organizzazioni di *marketing*.

# CAPITOLO 2

# LA TUTELA DELLA RISERVATEZZA E LA PROTEZIONE DEI DATI PERSONALI

**SOMMARIO:** 1. Introduzione – 2. Il diritto alla privacy: dal right to be left alone alla data protection – 3. L'avvento del Regolamento Europeo 2016/679 – 4. Le autorità di controllo – 5. Le direttive gemelle: novità sui contenuti e servizi digitali e sui contratti di vendita ai consumatori – 6. Il nuovo approccio europeo all'intelligenza artificiale – 7. Nuovi fenomeni lesivi della riservatezza e problemi di tutela del diritto alla protezione dei dati personali – 8. Data privacy e data security nel marketing.

## 1. Introduzione

Le imprese oggigiorno devono affrontare due tendenze: (1) la crescente pressione dei requisiti normativi in materia di protezione dei dati personali che sta emergendo in tutto il mondo; (2) la crescente consapevolezza dei diritti alla *privacy*, che induce i clienti ad agire nei loro rapporti con le imprese. La *privacy* dei dati è più di una semplice conformità o un problema aziendale. Le persone diventano vulnerabili ogni volta che consegnano le loro informazioni personali. Le imprese, indipendentemente dal settore, devono ai propri clienti la protezione delle proprie informazioni personali come se stessero proteggendo i beni più preziosi delle persone. I consumatori richiedono sempre più protezione e controllo sui propri dati. Le imprese che associano la *privacy* al proprio *brand* e la

abbracciano come responsabilità sociale ispirano maggiore fiducia ai clienti. L'approccio di un'impresa alla *privacy* dipende dalle prospettive morali dei *leader*. La prospettiva etica del *top management* determina se una impresa sarà proattiva nell'impostazione e supporto delle politiche di protezione dei dati. Le imprese possono scegliere di concentrarsi sulla conformità al minimo costo possibile, giocando al passo con le autorità di regolamentazione e offrendo al contempo un'esperienza mediocre per i clienti, oppure possono sfruttare la conformità per stimolare la cultura aziendale e identificare la *privacy* come uno dei valori fondamentali dell'organizzazione. Certo è che l'impegno per la *privacy* richiede più di un semplice *marketing tag-line*. Senza un impegno reale e tangibile per la *privacy* dei clienti, le organizzazioni continueranno a non essere all'altezza e i clienti attenti se ne accorgeranno e se ne andranno. L'approccio alla protezione dei dati come strategia di *core business* e iniziativa di CSR, piuttosto che un problema di sicurezza o di *information technology*, si distinguerà come un attraente fattore di differenziazione competitivo delle imprese rispetto ad altre che evitano la sicurezza dei dati o consentono volontariamente di acquistare, vendere e utilizzare i dati degli utenti privati.

## 2. Il diritto alla privacy: dal right to be left alone alla data protection

La nozione di *privacy* non può dirsi unificante[111]. Inizialmente riferito alla sfera della vita privata di una persona nella accezione di "riservatezza", nel tempo il

[111] NIGER S. (2006), *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, Padova, p. XI, cit.

significato di *privacy* è stato sottoposto a un'interpretazione estensiva in relazione all'evoluzione tecnologica intercorsa, arrivando dunque ad indicare il diritto al controllo sui propri dati personali, fino a giungere a comprendere l'identità personale[112]. La posizione più autorevole che esista una sfera intangibile dell'individuo riguardante la sua vita privata risale ad Aristotele che propose una distinzione ormai classica fra la sfera pubblica, connessa all'attività politica intesa col corrispondente greco di *Polis*, e la sfera privata, *Oikos*, associata alla famiglia ed alla vita domestica. Quest'ultima è ben riassunta nelle parole che William Pitt, The Elder Lord Chatham, pronunciò nel 1766 di fronte al Parlamento inglese in un dibattito sull'uso delle garanzie costituzionali: «[...] il più povero degli uomini può, nella sua casetta lanciare una sfida opponendosi a tutte le forze della corona. La casetta può essere fragile, il suo tetto può essere traballante, il vento può soffiare da tutte le parti, la

[112] BALDASSARRE A. (1997), *Diritto della persona e valori costituzionali*, G. Giappichelli Editore, Torino, passim; BILOTTA F. (1999), *L'emersione del diritto alla privacy*, in CLEMENTE A. (a cura di), *Privacy*, Cedam, Padova, p. 54 ss.; BUTTARELLI G. (1997), *Banche dati e tutela della riservatezza*, Giuffrè Editore, Milano, passim; COLAIANNI N. (2000), *Tutela della personalità e diritti della coscienza*, Cacucci Editore, Bari, passim; FRANCESCHELLI V. (1998), *La tutela della privacy informatica: problemi e prospettive*, Giuffrè Editore, Milano, passim; GIANNANTONIO E., LOSANO G., ZENO-ZENCOVICH V. (a cura di) (1999), *La tutela dei dati personali. Commentario alla legge n. 675/96*, seconda edizione, Cedam, Padova, passim; PARDOLESI R. (a cura di) (2003), *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè Editore, Milano, 2003, passim; RODOTÀ S. (1997), *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, Rivista critica del diritto privato, 4, pp. 583 ss.; ID. (1991), *Privacy e costruzione della sfera privata. Ipotesi e prospettive*, Politica del diritto, XXII, pp. 525 ss.; ID. (1995), *Tecnologie e diritti*, Il Mulino, Bologna, pp. 106 ss.; ID. (1997), *Controllo e riservatezza a garanzia della privacy ma senza i "lacci" della Burocrazia*, Guida al Diritto, pp. 10-14.

tempesta può entrare e la pioggia può entrare, ma il re d'Inghilterra non può entrare; tutte le sue forze non osano attraversare la soglia di tale casetta in rovina»[113]. Ma le origini moderne, dal punto di vista dottrinale, risalgono a fine Ottocento: «[…] I mutamenti politici, sociali ed economici obbligano al riconoscimento di nuovi diritti»[114]: così scrivevano nel 1890 Warren e Brandeis nell'articolo che, ancora oggi, viene ritenuto il fondamento del *right of privacy*[115]. Il diritto alla riservatezza nasceva così nel *Common Law*, come reazione alle indiscrezioni dell'*Evening Gazette* di Boston sulle amicizie della signora

---

[113] PITT W., THE ELDER LORD CHATHAM, discorso del marzo 1766, citato in HENRY PETER BROUGHAM, Historical Sketches of statesmen Who Flourished in the Time of George III, Charles Knights & Co, Londra, 1839, vol. 1, p. 52: "*The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail—its roof may shake—the wind may blow through it—the storm may enter—the rain may enter—but the King of England cannot enter!—all his force dares not cross the threshold of the ruined tenement!*".

[114] BRANDEIS L.D., WARREN S. (1890), *The Right to Privacy*, Harward Law Review, 4, pp. 193- 220. Citazione divenuta ormai obbligatoria in quanto il saggio ebbe il merito di avviare una vera e propria rivoluzione giuridica e sistematica sul concetto di *privacy*. Così gli autori scrivevano nelle prime righe del loro articolo: «*Recent inventions and business methods call attention to the next step which must be taken for the protection of the person… Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life…».*

[115] Diritto che due anni prima, nel 1888, il giudice Thomas Cooley, giudice supremo della suprema corte del Michigan fra il 1864 ed il 1885, aveva definito *the right to be let alone* (diritto ad essere lasciati soli). COOLEY T. C., *A Treatise on the Law of Torts or the Wrongs which Arise Independent of Contract*, Callaghan & Company, Chicago, IL, 1888, p. 29. In realtà la citazione "*the right to be let alone*" è tratta dalla prefazione alla seconda edizione dell'opera di Cooley, che fu scritta ancor prima, nel 1879 in seguito ad un caso giurisprudenziale riscontrato dallo stesso giudice supremo.

Warren e sulle nozze della figlia di Warren[116]. Gli autori nel loro saggio analizzavano in maniera approfondita le relazioni intercorrenti tra riservatezza da riconoscere ad un individuo, il diritto della stampa ad informare e al contempo quello dei cittadini ad essere informati. I nuovi profili che andava ad assumere la stampa, proiettandosi in un'ottica commerciale, con strategia di impresa, erano i principali segnali d'allarme per il "sacro spazio della vita privata e domestica" dell'individuo. La capacità del giornalismo d'impresa di diffondere in maniera rapida e ampia una notizia, insieme ad un sempre maggiore utilizzo dello strumento fotografico a supporto del contenuto scritto, ha fatto sì che anche fatti puramente mondani, fossero pietanza prelibata per l'insaziabile curiosità della borghesia bostoniana dell'Ottocento. Diventavano così di dominio pubblico fatti riguardanti non solo cittadini che non avevano specifiche responsabilità pubbliche, ma vicende che non avevano alcun tipo di rilevanza pubblica o comunque tali da giustificare gli ampi spazi dedicati dalle testate giornalistiche dell'epoca o un controllo così incessante[117]. La vera innovazione nella definizione di

[116] Samuel D. Warren e Louis D. Brandeis erano due giovani avvocati. Il primo, dopo aver sposato la figlia di un senatore, aveva cominciato a condurre una vita all'insegna del lusso sfrenato e ciò attirò l'attenzione dei giornali, che con i loro articoli "piccanti" suscitarono un grande scandalo. Warren, irritato da tanta e tale invadenza nella sua vita privata, colse l'occasione per scrivere con un suo vecchio compagno di studi dell'università, Brandeis, un saggio intitolato "*The Right to Privacy*". Secondo gli autori, "ognuno ha diritto di essere lasciato in pace, di proteggere quella che è la sfera più intima, così come ha diritto di proteggere, e difendere, da altrui invasioni, la sua proprietà privata".

[117] Il contesto storico non è casuale: la nascita della stampa a rotativa e della fotografia moderna sono causa della forte rivoluzione industriale del XIX secolo, propria di un balzo verso la modernità senza

*privacy* arriva nel 1967 a opera di Alan Westin, che cercando di delineare dei confini al valore della riservatezza, fornisce una definizione attuale, spezzando le catene di quella posizione ottocentesca imperniata sul modello giuridico della proprietà privata[118], per la quale «[…] la *privacy* è riconosciuta pienamente come diritto e anche potere che scaturisce da un insindacabile atto di volontà. È una pretesa legittima che ogni individuo ha di decidere in che misura e in che modo vuole condividere una parte di sé con gli altri. *Privacy* è sinonimo del diritto d'essere lasciato solo, definita anche come relazione zero fra due o più persone nel senso che non c'è interazione fra loro se decidono così. Ma l'uomo vive in una comunità ed ha anche la necessità di partecipare e comunicare dunque quando questo aspetto della *privacy* a due lati si scontra col potere riconosciuto del governo di funzionare per il benessere pubblico, ben si motiva la problematica recente sulle invasioni e intrusioni nella *privacy* individuale»[119]. I diritti hanno un fondamento storico e nascono e si trasformano in corrispondenza del mutamento delle

precedenti e figlia, a sua volta, delle rivoluzioni a cavallo fra il XVIII ed il XIX secolo.

[118] In origine, prima ancora che Warren e Brandeis teorizzassero il diritto alla *privacy* come *the right to be let alone*, e dunque come diritto alla riservatezza, la tutela della sfera privata era sostanzialmente legata alla tutela del diritto di proprietà: la protezione della vita privata si aveva fin dove si estendeva la proprietà dell'abitazione del titolare con divieto correlato per i terzi di intromettervisi senza il consenso del proprietario.

[119] WESTIN A. F. (1967), *Privacy and Freedom*, New York: Atheneum, First Edition. È ampiamente considerato il primo lavoro significativo sul problema della *privacy* dei consumatori e della protezione dei dati che ha ispirato la legislazione sulla *privacy* degli Stati Uniti e ha contribuito a lanciare movimenti globali per la *privacy* in molte nazioni democratiche negli anni '60 e '70.

condizioni storiche, economiche e sociali[120]: il diritto alla *privacy* nasce come esigenza morale e diventa diritto in senso giuridico in epoca moderna, trasformandosi da enunciazione di principio a diritto esigibile nel momento in cui viene disciplinata da specifiche leggi, che vengono emanate nei vari paesi in tempi diversi, prima con riferimento alla tutela della riservatezza poi – dopo la rivoluzione tecnologica – con riferimento al diritto alla protezione dei dati personali o alla cosiddetta *privacy* elettronica[121]. Nell'era digitale, i dati personali sono descritti come «nuovo petrolio» o «nuovo oro»[122]. In Europa, il primo provvedimento volto a introdurre una normativa precisa relativa alla protezione e al corretto trattamento dei dati personali – seguendo una direzione in parte già tracciata con la Convenzione di Strasburgo[123] n.

[120] Cfr. l'ampia riflessione di BOBBIO N. (1990), *L'età dei diritti*, Giulio Einaudi Editore, Torino, passim; per l'evoluzione successiva, fino all'attuale elaborazione concettuale di tale diritto, cfr., nella dottrina italiana, RODOTÀ S. (1995), *Tecnologie e diritti*, il Mulino, Bologna, passim; ID. (1997), *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, Rivista critica del diritto privato, 4, p. 583 ss.; ALPA G. (1998), *La disciplina dei dati personali: note esegetiche sulla Legge 31 dicembre 1996, n. 675 e successive modifiche*, Seam Edizioni, Roma, passim.

[121] FARALLI C. (2019), *Il diritto alla privacy. Profili storico-filosofici*, in ZORZI GALGANO N. (a cura di) (2019), *Persona e mercato dei dati. Riflessione sul GDPR,* Cedam, Padova, p. 4.

[122] THE ECONOMIST (2017), *Data is giving rise to a new economy - Fuel of the future*. Disponibile *online* al seguente indirizzo *world wide web*: https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy. Data di ultima consultazione: 21 luglio 2020.

[123] La Convenzione di Strasburgo del 1981, o anche Convenzione 108 del Consiglio d'Europa, è uno dei più importanti strumenti legali per la protezione delle persone rispetto al trattamento automatizzato dei dati personali.

108 del 1981 – è la Direttiva 95/46/CE[124], che fissa il principio che il trattamento dei dati è legittimo se è consentito dall'individuo che ne deve essere messo a conoscenza. Essa rappresenta l'esito di un percorso cominciato a livello europeo nella giurisprudenza della Corte EDU[125], che aveva rilevato che nell'ambito dell'art. 8 della CEDU, *Diritto al rispetto della vita privata e familiare* rientra anche la protezione dei dati personali[126], così come espressamente sottolineato nel *considerando* n. 10 della Direttiva[127]. La «Direttiva madre» in materia di

[124] 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.

[125] La Corte europea dei diritti dell'uomo (abbreviata in CEDU o Corte EDU) è un organo giurisdizionale internazionale, istituita nel 1959 dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) del 1950, per assicurarne l'applicazione e il rispetto.

[126] Art. 8 CEDU. Diritto al rispetto della vita privata e familiare: 1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.

[127] Considerando n. 10 Direttiva 95/46/CE: (10) considerando che le legislazioni nazionali relative al trattamento dei dati personali hanno lo scopo di garantire il rispetto dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata, riconosciuto anche dall'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e dai principi generali del diritto comunitario; che pertanto il ravvicinamento di dette legislazioni non deve avere per effetto un indebolimento della tutela da esse assicurata ma deve anzi mirare a garantire un elevato grado di tutela nella Comunità.

*privacy* è stata recepita in Italia con la legge n. 675 del 31 dicembre 1996[128] e ha delineato il diritto all'identità personale come diverso e distinto diritto rispetto al diritto alla riservatezza. Sulla stessa linea evolutiva si colloca il decreto legislativo n. 196 del 30 giugno 2003[129], il c.d. codice della *privacy*, che riconosce accanto al diritto alla riservatezza un autonomo diritto alla protezione dei dati personali, visione poi confermata dalla Carta dei Diritti Fondamentali dell'Unione Europea[130], formata a Nizza nel 2000 e dal 2009 divenuta parte integrante del Trattato di Lisbona nella quale all'art. 8 si fa esplicito riconoscimento al diritto alla protezione dei dati personali[131].

---

[128] Legge n. 675 del 31 dicembre 1996, Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali (testo consolidato con il d.lgs. 28 dicembre 2001, n. 467) (Pubblicato sulla Gazzetta Ufficiale n. 5 dell´8 gennaio 1997 - Suppl. Ordinario n. 3) Legge abrogata ai sensi dell'articolo 183, comma 1, lettera a), del Codice in materia di protezione dei dati personali.

[129] Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" pubblicato nella Gazzetta Ufficiale n. 174 del 29 luglio 2003 - Supplemento Ordinario n. 123.

[130] La Carta dei diritti fondamentali dell'Unione europea (CDFUE), in Italia anche nota come Carta di Nizza, è stata solennemente proclamata una prima volta il 7 dicembre 2000 a Nizza e una seconda volta, in una versione adattata, il 12 dicembre 2007 a Strasburgo da Parlamento, Consiglio e Commissione. Con l'entrata in vigore del "Trattato di Lisbona", la Carta di Nizza ha il medesimo valore giuridico dei trattati, ai sensi dell'art. 6 del Trattato sull'Unione europea, e si pone dunque come pienamente vincolante per le istituzioni europee e gli Stati membri e, allo stesso livello di trattati e protocolli ad essi allegati, come vertice dell'ordinamento dell'Unione europea. Essa risponde alla necessità, emersa durante il Consiglio europeo di Colonia (3 e 4 giugno 1999), di definire un gruppo di diritti e di libertà di eccezionale rilevanza e di fede che fossero garantiti a tutti i cittadini dell'Unione.

[131] Art. 8 Carta dei diritti dell'Unione europea (Carta di Nizza): 1. Ogni persona ha diritto alla protezione dei dati di carattere personale

## 3. L'avvento del Regolamento Europeo 2016/679

Nell'ambito degli strumenti normativi previsti dal Trattato sul Funzionamento dell'Unione Europea, il Regolamento, a differenza della Direttiva, della Decisione, della Raccomandazione e del Parere, è la misura maggiormente penetrante negli ordinamenti giuridici dei singoli Stati membri. Difatti, come sancisce l'art. 288 TFUE, il Regolamento ha portata generale, inerendo agli Stati membri e a tutti i soggetti giuridici dell'Unione; è obbligatorio in tutte le sue parti, vincolando gli Stati membri sia sotto il profilo delle finalità, sia dal punto di vista dei mezzi da utilizzare per il conseguimento degli obiettivi; è direttamente applicabile dalla data di entrata in vigore[132]. Gli effetti giuridici sono simultaneamente, automaticamente e uniformemente vincolanti in tutte le legislazioni nazionali. Il Regolamento rientra nel diritto secondario dell'Unione Europea e si rivolge a categorie astratte di persone, non a specifici individui. È un atto giuridico adottato dal Consiglio e dal Parlamento secondo

che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

[132] Cfr. Trattato sul funzionamento dell'Unione Europea (TFUE), art. 288: Per esercitare le competenze dell'Unione, le istituzioni adottano regolamenti, direttive, decisioni, raccomandazioni e pareri. Il regolamento ha portata generale. Esso è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri. La direttiva vincola lo Stato membro cui è rivolta per quanto riguarda il risultato da raggiungere, salva restando la competenza degli organi nazionali in merito alla forma e ai mezzi. La decisione è obbligatoria in tutti i suoi elementi. Se designa i destinatari è obbligatoria soltanto nei confronti di questi. Le raccomandazioni e i pareri non sono vincolanti.

procedure legislative ordinarie o speciali. Il 25 maggio 2018 è iniziata ufficialmente l'era del *General Data Protection Regulation* (GDPR)[133], vale a dire il sistema normativo composto da 99 articoli e 173 *considerando* che definisce il quadro giuridico comune in materia di protezione dei dati personali per tutti gli Stati membri della Unione Europea con l'obiettivo di uniformare e armonizzare la suddetta disciplina, eliminando le svariate asimmetrie che nel corso del tempo si sono create con le normative nazionali frammentarie e diverse tra loro. Per anni tali barriere hanno difatti ostacolato la libera circolazione dei dati tra una nazione e l'altra, causando la penalizzazione sullo sviluppo del mercato unico digitale. Il Regolamento europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione dai dati, il c.d. *General Data Protection Regulation* (GDPR), raccoglie l'importante eredità della Direttiva 95/46/CE, ma a differenza di quest'ultima, che era fondata su un approccio autorizzatorio, è fondato sul principio della *accountability*, ossia della responsabilità[134]: ciò significa che il titolare del

[133] Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la dir. 95/46/CE (Regolamento generale sulla protezione dei dati). A completamento della materia dei dati si consideri il Reg. (UE) 2018/1807 del Parlamento europeo e del Consiglio del 14 novembre 2018 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, nonché, in ultimo, la dir. (UE) 2018/1972 del Parlamento europeo e del Consiglio dell'11 dicembre 2018, da attuarsi entro il 21 dicembre 2020, che istituisce il codice europeo delle comunicazioni elettroniche e che tocca, con disposizioni specifiche, anche l'ambito dei dati di carattere personale.

[134] Cfr. Gruppo di lavoro Articolo 29 per la protezione dei dati, parere 3/2010 sul principio di responsabilità, adottato il 3 luglio 2010,

trattamento deve essere in grado di dimostrare che ha adottato un complesso di misure giuridiche e tecniche per la protezione dei dati[135]. Lo scopo e le due anime del Regolamento[136] si evincono dall'art. 1: la volontà del legislatore storico è in primo luogo la protezione delle persone fisiche (diversa dalla protezione dei dati personali) con riguardo al trattamento dei dati e in secondo luogo la

punto 10, nonché punto 16, in cui si sottolinea che il principio di responsabilità non è una novità in sé, ma è ravvisabile nelle linee guida per la protezione della vita privata dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) adottato nel 1980, nonché inserito esplicitamente anche tra gli *standard* internazionali di Madrid elaborati dalla conferenza internazionale sulla protezione dei dati e la *privacy*, nonché accolto in sede internazionale. Cfr. anche Parere 3/2010, punto 35: "Alcuni responsabili del trattamento potrebbero percepire il principio generale di responsabilità come un'onerosa imposizione di nuovi obblighi giuridici in capo ai responsabili al trattamento, in particolare vista l'attuale difficile situazione economica dell'UE. Questa interpretazione non sarebbe corretta".

[135] MANTELERO A. (2017), *Responsabilità e rischio nel Reg. UE 2016/679*, Le Nuove leggi civili commentate, 1, p. 144 e ss.; CALIFANO L., COLAPIETRO C. (a cura di) (2017), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale Scientifica, Napoli; FINOCCHIARO G. D. (2017), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli Editore, Bologna.

[136] Cfr. art. 1 del GDPR: 1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati. 2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali. 3. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

libera circolazione dei dati[137]. Dunque, la protezione delle persone è un diritto assoluto e si distingue dal diritto di protezione dei dati; il diritto alla protezione dei dati non è una prerogativa assoluta e va bilanciato con altri diritti prerogativa di soggetti pubblici e soggetti privati, tra cui la libertà d'impresa[138]. Pertanto, anche il diritto a trattare dati non è una prerogativa assoluta[139]. Il Regolamento UE 2016/679 prende atto del mutamento tecnologico e sociale degli ultimi vent'anni, che ha reso sempre più i dati un bene giuridico economicamente valutabile, come esplicitato dal *considerando* nr. 6[140]. Da ciò deriva la necessità di creare un quadro più solido e coerente in materia di *privacy*, ma

[137] Cfr. considerando nr. 1 del GDPR: La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

[138] Cfr., per una ricostruzione organica, BRAVO F. (2018), *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Cedam, Padova.

[139] BERNARDI N., CICCIA MESSINA A. (2017), *Privacy e Regolamento Europeo*, IPSOA, Milano, p. 7

[140] Cfr. considerando nr. 6 del GDPR: La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che le riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.

anche di considerare la protezione dei dati personali come oggetto di possibili bilanciamenti, secondo quanto espressamente indicato nel *considerando* nr. 4[141]. Il nuovo Regolamento ha consolidato il quadro dei diritti e lo ha ampliato, introducendone nuovi, tra i quali: (a) il diritto alla portabilità dei dati, che consente all'interessato di ricevere i dati che lo riguardano forniti a un titolare del trattamento e di trasmetterli ad altro titolare anche al fine di evitare usi diversi rispetto a quelli dichiarati; (b) il diritto di opposizione, che permette di opporsi al trattamento dei dati con particolare riferimento alla profilazione, che attraverso tecniche e algoritmi sempre più raffinati costruisce un profilo che misura le abitudini di consumo, gli interessi, le scelte e (c) il diritto all'oblio, che si riferisce alla possibilità di poter cancellare notizie rispetto alle quali è trascorso un notevole lasso di tempo. A livello nazionale, le nuove regole in materia di trattamento e libera circolazione dei dati personali sono entrate in vigore il 19 settembre 2018: è così stato recepito anche dall'Italia con il decreto legislativo 10 agosto 2018 n. 101[142] il Regolamento

[141] Cfr. considerando nr. 4 del GDPR: Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. 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. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.

[142] Decreto legislativo 10 agosto 2018, n. 101, Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio,

europeo 2016/679, che abroga la direttiva 95/46/CE. Il decreto legislativo n. 196 del 2003, ossia il vecchio Codice *privacy* non è stato abrogato totalmente[143]; difatti, il

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 (regolamento generale sulla protezione dei dati). (18G00129) (GU Serie Generale n.205 del 04-09-2018).

[143] L'art. 1 del Codice in materia di protezione dei dati personali (d. lgs. 196 del 2003 e ss.mm.ii.), nella sua originaria formulazione, chiariva che la finalità dell'intervento normativo era quella di garantire "che il trattamento dei dati personali si svolga nel rispetto dei diritti e della libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali". La norma, che esplicita per la prima volta nell'ordinamento giuridico italiano il diritto alla protezione dei dati personali, fa da eco all'art. 1, par. 1, della dir. 95/46/CE, ai sensi del quale "gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e della libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali". Precisa giustamente ZORZI GALGANO N. (2019), *Persona e mercato dei dati. Riflessione sul GDPR,* Cedam, Padova, p. 36 ss., che nell'ottica di accordare centralità alla persona a cui i dati si riferiscono il Codice assegna una posizione centrale al consenso al trattamento, che diviene predominante tra i presupposti di liceità del trattamento, mentre gli altri fondamenti legittimi appaiono vere e proprie eccezioni ad esso (v. art. 23 e 24 del Codice, fino alle modifiche del 2018 intervenute con il d. lgs. 101/2018, con cui è stata adeguata la disciplina nazionale a quella del GDPR). Si tratta, sempre secondo l'autore, di indici normativi volti a riconoscere una posizione di maggior protezione per la *privacy* rispetto agli altri due diritti. Al contrario, nel GDPR il legislatore europeo mostra invece di dare maggiore risalto anche all'altra anima della disciplina, quella della libera circolazione dei dati, che risulta rafforzata rispetto all'impianto della direttiva e delle norme interne di recepimento, in particolare a seguito del depotenziamento del consenso dell'interessato rispetto agli altri fondamenti legittimi, ora in posizione equivalente al consenso. Ne risulta non solo legittimato, ma anche rafforzato, rispetto al quadro precedente, il diritto al

legislatore ne ha armonizzato il contenuto, prevedendo in questo modo una abrogazione parziale[144]. Alla luce delle fonti e internazionali il diritto alla *privacy* odierno si delinea come fattispecie complessa, un diritto alla personalità che tiene al suo interno diritto alla riservatezza, diritto alla protezione dei dati personali e diritto all'identità personale[145]. Il legislatore non ha inteso meramente caricare di nuovi compiti il titolare del trattamento, quanto piuttosto coinvolgerlo in un processo volto a erogare beni e servizi *privacy oriented*, sulla base di un mutamento di prospettiva che intenda la protezione dei dati personali come valore (come *asset*) piuttosto che come costo,

trattamento e dunque la posizione anche autonomamente protetta del titolare del trattamento stesso.

[144] Cfr. CUFFARO V. (2018), *Quel che resta di un codice: il D.Lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del codice della privacy al regolamento sulla protezione dei dati*, Corriere giuridico, 10, p. 1181 e ss. A seguito dell'entrata in vigore del Regolamento, il Codice non rappresenta più un *corpus* normativo autonomo, ma è necessariamente complementare, se non proprio ancillare, al GDPR. Quest'ultimo ne costituisce idealmente la vera Parte generale, o Parte I, in sostituzione di quella oggi quasi completamente abrogata. In realtà la diretta applicabilità del Regolamento rendeva non necessaria l'abrogazione espressa operata dal d. lgs. n. 101, in quanto dal 25 maggio 2018, con la piena attuazione del Regolamento, erano già venute meno tutte le disposizioni interne con esso incompatibili. Tuttavia, tale atto di doverosa pulizia normativa, oltre a derivare da un preciso mandato del legislatore delegante, segna anche una presa di coscienza del salto di qualità realizzato e del passaggio ad una disciplina integralmente europea, che dispiega direttamente la sua forza nell'ordinamento interno. Cfr. BUSIA G. (2019), *Il ruolo dell'autorità indipendente per la protezione dei dati personali*, in ZORZI GALGANO N. (a cura di) (2019), *Persona e mercato dei dati. Riflessione sul GDPR,* Cedam, Padova, p. 296, nota a piè di pagina nr. 6.

[145] FARALLI C. (2019), *Il diritto alla privacy. Profili storico-filosofici*, in ZORZI GALGANO N. (a cura di) (2019), *Persona e mercato dei dati. Riflessione sul GDPR,* Cedam, Padova, p. 9.

delineando un compromesso di regole nel segno di un contemperamento tra i diritti dell'interessato e quello del titolare ad espletare il trattamento senza scontare il peso di adempimenti e costi sproporzionati rispetto al tipo di attività svolta[146].

### *3.1 Le figure del trattamento dei dati personali*

La complessità della protezione dei dati nella attuale era tecnologica richiede varie figure con diversi compiti, alcune previste dal Regolamento, altre derivano dalle necessità che le aziende riscontrano per riuscire a gestire correttamente i dati[147]. Il Regolamento Europeo 2016/679, all'art. 4, individua le figure del titolare del trattamento, del responsabile del trattamento, del rappresentante, e agli artt. 37 – 39 contempla il responsabile della protezione dei dati. 1. Il titolare del trattamento (*data controller*)[148]. L'art. 24

[146] BRAVO F. (2018), *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Cedam, Padova, suggerisce la lettura del sistema che attribuisce rilievo al potere/diritto del titolare a svolgere il trattamento; cfr. anche MOLLO F. (2019), *Gli obblighi previsti in funzione di protezione dei dati personali*, in ZORZI GALGANO N. (a cura di) (2019), op. cit., p. 256.

[147] BERNARDI N., CICCIA MESSINA A. (2017), *Privacy e Regolamento Europeo*, IPSOA, Milano, p. 88.

[148] Cfr. PIZZETTI F. (2016), *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, G. Giappichelli Editore, Torino, p. 55; ID. (2016), *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, G. Giappichelli Editore, Torino, p. 196 ss., nella traduzione italiana del Regolamento 2016/679 il termine inglese «*controller*» è tradotto con il termine di «titolare», in ossequio alla diversa terminologia nazionale italiana da tempo adottata nella legislazione interna. Una eccezione che è stata chiesta e ottenuta dal Garante italiano anche per evitare ulteriori confusioni. Resta fermo che nel Regolamento il termine inglese «*controller*» è tradotto con il

tratta della responsabilità del titolare. Avere la responsabilità significa esercitare prerogative a patire dalle conseguenze negative per il cattivo esercizio delle prerogative stesse. Si tratta di una sorta di principio di responsabilizzazione, secondo cui si chiede al titolare del trattamento di mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento. Le adesioni ai codici di condotta o ai meccanismi di certificazione aiutano a dimostrare la conformità al Regolamento. L'adeguatezza delle misure, valutata in base alla natura, all'ambito, al contesto, alle finalità e a probabilità e gravità dei rischi, deve essere dimostrata dal titolare del trattamento, implicando in tal maniera oneri formali e sostanziali. Il titolare è tenuto a precostituire un apparato documentale, dimostrando in senso formale di avere valutato tutti i possibili parametri della sua responsabilità. Inoltre, il titolare deve anche precostituire un apparato di misure che proteggono le persone, evitando che i dati siano sottratti o persi o se ne perdano le tracce o se ne faccia un uso sviato. 2. Il responsabile del trattamento (*data processor*). Ai sensi dell'art. 28, il responsabile è il soggetto che tratta dati personali per conto di un titolare del trattamento; può essere una persona fisica o giuridica, un'autorità pubblica o altro organismo. Il titolare del trattamento designa con un contratto il responsabile del trattamento sulla base di competenze. A sua volta il responsabile può designare un altro responsabile, alla condizione che vi sia

termine italiano «titolare» (non «responsabile», come invece è tradotto nella Direttiva 95/46). Egualmente il termine inglese «*processor*» è tradotto col termine italiano «responsabile» e non, come invece è nella Direttiva, col termine «incaricato». Quando si confrontano Direttiva e Regolamento occorre tener conto di queste differenze terminologiche.

l'autorizzazione scritta del titolare del trattamento. La designazione del responsabile deve contenere la materia disciplinata, 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. I rapporti tra titolare e responsabile o tra responsabile e altro responsabile sono di natura contrattuale. Di fronte al titolare il primo responsabile risponde di eventuali inadempimenti del secondo responsabile. Qualora vi siano delle violazioni, il responsabile del trattamento deve informare immediatamente il titolare. L'adesione a un codice di condotta o a un meccanismo di certificazione può essere utilizzata come elemento per dimostrare garanzie sufficienti di competenza e affidabilità. 3. I corresponsabili del trattamento (*joint controllers*). L'art. 26 del Regolamento prevede la contitolarità del trattamento, ossia quella situazione che si verifica quando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento. I contitolari devono stipulare un accordo sulle rispettive responsabilità, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni[149]. L'interessato può esercitare i propri diritti ai sensi del Regolamento nei confronti di e contro ciascun titolare del trattamento. 4. L'incaricato del trattamento. La figura dell'incaricato del trattamento era già prevista dal Codice della *privacy* italiano (d.lgs. n. 196/2003) come «la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile». Con il nuovo Regolamento europeo invece non è più espressamente prevista. Comunque sia, il Regolamento prevede per il titolare del trattamento l'obbligo di formare gli addetti autorizzati al

[149] Si pensi, ad esempio, al medico specialista che opera all'interno della struttura sanitaria, la quale archivia i dati del paziente: questo è un caso di contitolarità del trattamento.

trattamento dei dati. Chiunque agisce sotto l'autorità del titolare del trattamento o del responsabile, che abbia accesso a dati personali, quindi, non può trattare 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. 5. Infine, vi è la figura dell'interessato (*data subject*) al trattamento, ossia la persona fisica (e non giuridica, come chiarito dal *considerando* nr. 14 del GDPR) a cui si riferiscono i dati personali.

## 4. Le autorità di controllo

Al fine di assicurare un'applicazione corretta delle norme e pur scontando differenziazioni legate alle specifiche discipline nazionali, il nuovo Regolamento UE 2016/679 amplia (rispetto alla Direttiva 95/46) i poteri e i compiti delle Autorità nazionali di controllo. Ai sensi dell'art. 52, le Autorità nazionali di controllo godono di una posizione di indipendenza. La Sezione 2 del Capo VI attribuisce loro compiti e poteri molto incisivi. Le Autorità di controllo collaborano sia separatamente che congiuntamente con il Comitato europeo per la protezione dei dati.

### *4.1 Il Garante per la protezione dei dati personali*

Il Garante per la protezione dei dati personali (GPDP) è un'autorità amministrativa indipendente istituita dalla cosiddetta legge sulla *privacy* (legge 31 dicembre 1996, n. 675), poi disciplinata dal Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003 n. 196), come modificato dal Decreto legislativo 10 agosto 2018, n. 101. Quest'ultimo ha confermato che il Garante è l'autorità di

controllo designata anche ai fini dell'attuazione del Regolamento generale sulla protezione dei dati personali (UE) 2016/679 (art. 51). Nel corso degli anni vi è stato un progressivo rafforzamento del Garante *privacy* attraverso la normativa interna e sovranazionale. Il primo provvedimento è la Convenzione del Consiglio d'Europa n. 108 del 1981[150], che sebbene ne individui alcune funzioni, non faceva espresso riferimento all'istituzione di una autorità di controllo, come successivamente previsto

[150] Convenzione n. 108 per la protezione delle persone in relazione al trattamento automatizzato dei dati a carattere personale, adottata a Strasburgo il 28 gennaio 1981. La ratifica della Convenzione da parte dei singoli Stati presupponeva l'adozione di una disciplina interna sulla tutela dei dati personali (artt. 4 e 22). L'Italia, che pure aveva in precedenza autorizzato tale ratifica (l. n. 98/1998), non ha potuto per lungo tempo procedere al deposito dei relativi strumenti proprio per la mancanza di una legge sulla protezione dei dati personali. Grazie all'approvazione della l. 675/1996, è stato possibile adeguarsi agli *standard* di garanzia previsti dalla Convenzione, e così consentire la sua entrata in vigore a partire dal 1° luglio 1998. Il raggiungimento, attraverso il diritto interno, del livello di tutela previsto dalla Convenzione era infine legato anche alla piena applicazione dell'Accordo di Schengen, mirante a creare uno spazio comune per la libera circolazione delle persone e delle merci, attraverso la progressiva soppressione dei controlli alle frontiere (mentre l'autorizzazione alla ratifica dell'Accordo di Schengen del 14 giugno 1985 era stata resa dall'Italia con la l. n. 338/1993). La Convenzione è stata oggetto di un lungo processo di ammodernamento, legato alla approvazione del GDPR, che ha comportato una prima definizione di un testo, approvato sul piano tecnico nel 2016, da parte di un apposito Comitato (CAHDATA) e che si è conclusa il 18 maggio 2018 con l'adozione da parte del Comitato dei ministri in occasione della sua 128ª sessione svoltasi a Elsinore, e con la successiva sottoscrizione da parte di diversi Paesi tra i quali anche l'Italia, sebbene con leggero ritardo. Cfr. BUSIA G. (2019), *Il ruolo dell'autorità indipendente per la protezione dei dati personali*, in ZORZI GALGANO N. (a cura di) (2019), *Persona e mercato dei dati. Riflessione sul GDPR,* Cedam, Padova, p. 299, nota a piè di pagina nr. 12.

dal suo Protocollo addizionale dell'8 novembre 2001, firmato ma non ratificato dall'Italia. Un rilevante riferimento emerge dall'Accordo di Schengen[151] del 14 giugno 1985, ove si prevede la creazione di istanze indipendenti per il controllo dei dati personali elaborati sulla base di tale intesa. Tuttavia, il Garante *privacy* viene introdotto nell'ordinamento nazionale solo dall'art. 30 della l. n. 675/1996 di recepimento della dir. 95/46/CE, che richiedeva l'istituzione nei singoli Stati membri di una o più autorità di controllo pienamente indipendente, dotate di poteri investigativi, di intervento e consultivi nel processo di elaborazione normativa secondaria (art. 28). Successivamente, al fine di riordinare la materia sparsa nei numerosi decreti legislativi emanati successivamente e nella serie di disposizioni di rango inferiore, che nel complesso costituivano un insieme di norme di difficile interpretazione, la l. n. 675/1996 è stata sostituita[152] a

[151] L'Accordo di Schengen (ufficialmente Accordo fra i governi degli Stati dell'Unione economica del Benelux, della Repubblica federale di Germania e della Repubblica francese relativo all'eliminazione graduale dei controlli alle frontiere comuni) è un trattato internazionale firmato a Schengen il 14 giugno 1985 tra Benelux, Germania Ovest e Francia, che prevedeva la creazione di uno spazio comune, tramite una progressiva eliminazione dei controlli alle frontiere comuni tra i cinque Stati interessati, sia delle merci sia delle persone. L'accordo è stato il primo passo del cosiddetto *acquis* di Schengen, che dal 1999 è stato integrato nel quadro istituzionale e giuridico dell'Unione Europea.

[152] Il 31 dicembre 1996, nella medesima data della l. n. 675/1996, venne adottata la l. n. 676/1996, con la quale si delegava il Governo ad emanare disposizioni integrative della legislazione in materia, al fine di rimediare alla parziale incompletezza della legge n. 675, la cui elaborazione aveva scontato l'urgenza di adottare in tempo utile le disposizioni necessarie a consentire la partecipazione dell'Italia allo "spazio Schengen". Precisa BUSIA G. (2019), *Il ruolo dell'autorità indipendente per la protezione dei dati personali*, in ZORZI GALGANO N. (a cura di) (2019), *Persona e mercato dei dati. Riflessione sul GDPR,* Cedam, Padova, p. 300, "con due impianti normativi coevi in realtà

partire dal 1° gennaio 2004 dal c.d. Codice *privacy*, il cui art. 153 riproduceva il regime previgente del Garante. Nel frattempo, le autorità di controllo sulla protezione dei dati personali sono state costituzionalizzate e hanno trovato consacrazione nell'art. 8 della Carta dei diritti fondamentali dell'Unione Europea, poi recepito dal Trattato di Lisbona trovando conferma nell'art. 16 TFUE. Infine, con il Regolamento UE 2016/679 è stato imposto a tutti gli Stati membri l'istituzione di una autorità di controllo, enumerandone esaustivamente le caratteristiche necessarie a salvaguardarne l'indipendenza, requisito imprescindibile per il legislatore europeo (artt. 51-54), così come è stata prevista la sua introduzione con analoghi requisiti di terzietà (artt. 41-44) anche nel settore attinente alle attività di polizia e giustizia, con la direttiva 2016/680/UE[153]. Il Garante *privacy* è un organo collegiale

---

erano state poste le fondamenta per un'opera di manutenzione legislativa continua in un settore, quello della tutela dei dati personali, per sua natura in perenne evoluzione. Una legislazione statica e ferma al momento della sua adozione avrebbe invece rischiato di rendere immediatamente obsoleta la l. n. 675. La stessa lungimiranza legislativa si rinviene nel Regolamento, che presenta alcune clausole aperte, come, fra tutte, l'art. 97, ai sensi del quale la Commissione europea se del caso presenta proposte legislative di modifica di altri atti legislativi dell'Unione Europea, allo scopo di garantire una protezione uniforme e coerente in materia".

[153] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio. La direttiva richiede agli Stati membri di incaricare ad "autorità pubbliche indipendenti" la sorveglianza della sua corretta applicazione, potendo essi altresì disporre "che un'autorità di controllo istituita ai sensi del Regolamento (UE) 2016/679 sia l'autorità di controllo di cui alla […] Direttiva e assolva i

composto da quattro membri eletti dai due rami del Parlamento della Repubblica Italiana – che ne individuano due ciascuno – e le candidature possono essere avanzate da persone che assicurino indipendenza e che risultino di comprovata esperienza nel settore della protezione dei dati personali, con particolare riferimento alle discipline giuridiche o dell'informatica; in aggiunta, devono pervenire almeno trenta giorni prima della nomina e i *curricula* devono essere pubblicati negli stessi siti *internet*. I componenti eleggono nel loro ambito un presidente, il cui voto prevale in caso di parità; eleggono altresì un vicepresidente, che assume le funzioni del presidente in caso di sua assenza o impedimento. L'incarico di presidente e quello di componente hanno durata settennale e non sono rinnovabili. Per tutta la durata dell'incarico il presidente e i componenti non possono esercitare, a pena di decadenza, alcuna attività professionale o di consulenza, anche non remunerata, né essere amministratori o dipendenti di enti

compiti dell'autorità di controllo da istituirsi" (art. 41), fermo restando pur sempre l'applicazione del Regolamento ai trattamenti effettuati per finalità che esulano quelle specificatamente individuate in tale peculiare settore (cfr. considerando nr. 11, 12, 34, e 68). Nel lasciare agli Stati membri la scelta in ordine all'organismo deputato alla sorveglianza sul trattamento effettuato a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, la Direttiva non escludeva che, in sede di recepimento, tale compito possa essere attribuito al Garante e difatti tale è stata la scelta poi compiuta dal d. lgs. 18 maggio 2018, n. 51, recante Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU Serie Generale n. 119 del 24-05-2018). Cfr. art. 2, comma 1, lett. s).

pubblici o privati, né ricoprire cariche elettive[154]. Il Garante si occupa[155], tra l'altro, di controllare che i trattamenti di dati personali siano conformi al Regolamento nonché a leggi e regolamenti nazionali e prescrivere, ove necessario, ai titolari o ai responsabili dei trattamenti le misure da adottare per svolgere correttamente il trattamento nel rispetto dei diritti e delle libertà fondamentali degli individui; collaborare con le altre autorità di controllo e prestare assistenza reciproca al fine di garantire l'applicazione e l'attuazione coerente del Regolamento; esaminare reclami; (nel caso di trattamenti che violano le disposizioni del Regolamento) rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento e ingiungere di conformare i trattamenti alle disposizioni del Regolamento; imporre una limitazione provvisoria o definitiva del trattamento, incluso il divieto di trattamento; ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento; adottare i provvedimenti

[154] Cfr. art. 153 "Garante per la protezione dei dati personali" del Codice della *privacy*. L'attuale Collegio è stato eletto dal Parlamento il 14 luglio 2020 e si è insediato il 29 luglio 2020. Le nomina di Ginevra Cerrina Feroni (vicepresidente) e Guido Scorza (componente) sono state comunicate dalla Camera dei Deputati al Garante per la protezione dei dati personali in data 14 luglio 2020; le nomine di Pasquale Stanzione (presidente) e Agostino Ghiglia (componente) sono state comunicate dal Senato della Repubblica al Garante per la protezione dei dati personali in data 15 luglio 2020.

[155] I compiti del Garante sono definiti dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196), adeguato alle disposizioni del Regolamento (UE) 2016/679 tramite il Decreto legislativo 10 agosto 2018, n. 101, oltre che da vari altri atti normativi italiani e internazionali. Nel testo si riporta la scheda di sintesi redatta dall'Ufficio del Garante a puro scopo divulgativo. Per un quadro completo della materia si rimanda alla legislazione in tema di protezione dei dati personali.

previsti dalla normativa in materia di protezione dei dati personali; segnalare, anche di propria iniziativa, al Parlamento e altri organismi e istituzioni l'esigenza di adottare atti normativi e amministrativi relativi alle questioni riguardanti la protezione dei dati personali; formulare pareri su proposte di atti normativi e amministrativi; partecipare alla discussione su iniziative normative con audizioni presso il Parlamento; predisporre una relazione annuale sull'attività svolta e sullo stato di attuazione della normativa sulla *privacy* da trasmettere al Parlamento e al Governo; partecipare alle attività dell'Unione Europea ed internazionali di settore, anche in funzione di controllo e assistenza relativamente ai sistemi di informazione Europol, Schengen, VIS, e altri; curare l'informazione e sviluppare la consapevolezza del pubblico e dei titolari del trattamento in materia di protezione dei dati personali, con particolare attenzione alla tutela dei minori; tenere registri interni delle violazioni più rilevanti e imporre sanzioni pecuniarie ove previsto dal Regolamento e dalla normativa nazionale; coinvolgere, ove previsto, i cittadini e tutti i soggetti interessati con consultazioni pubbliche dei cui risultati si tiene conto per la predisposizione di provvedimenti a carattere generale. Per ciò che concerne gli adempimenti legati al principio di responsabilizzazione del titolare, il pacchetto europeo di protezione dati ha opportunamente eliminato il precedente obbligo di notificazione dell'avvio di ogni trattamento, che in Italia era stato via via circoscritto ai trattamenti più rischiosi[156] e ha esteso l'obbligo di notificazione alle

[156] L'obbligo di notificazione del trattamento, introdotto dalla dir. 95/46/CE e poi recepito in particolare nel Codice agli artt. 37 e ss., non aveva sempre contribuito a migliorare la protezione dei dati personali. Difatti, già nel passaggio dalla l. n. 675 del 1996 al Codice *privacy*, il legislatore, su impulso del Garante, aveva semplificato tale adempimento, rendendolo non più generalizzato, bensì relativo solo a

autorità di controllo delle violazioni di dati personali (art. 4, par. 1, p.12 del GDPR). In ragione di questo, il titolare è tenuto a notificare ogni violazione di dati personali per consentire all'autorità di individuare i rimedi necessari a limitare le conseguenze dell'evento, che verrà annotato in un apposito registro (artt. 33, 34, 37, 39, 57 e 58 del GDPR)[157]. La nuova normativa europea ha invece introdotto nuovi meccanismi, quale la valutazione d'impatto *privacy* a cura del titolare con la quale si richiede di ponderare la necessità del trattamento e i potenziali pericoli che ne possono derivare, individuando le misure più appropriate per affrontarli adeguatamente. In questo contesto, le autorità nazionali elaborano un elenco dei trattamenti che, in ragione dei rischi che possono presentare, devono essere previamente assoggettati a una valutazione d'impatto e sono tenute a rilasciare il proprio parere in caso di consultazione preventiva formulata dal titolare per trattamenti che profilano rischi talmente elevati da non essere fronteggiabili con la tecnologia disponibile (artt. 35, 36, e 57 del GDPR). In aggiunta, sono stati istituiti meccanismi di certificazione della protezione dei dati, al fine di migliorare la trasparenza e il rispetto del Regolamento UE 2016/679. I meccanismi di certificazione della protezione dei dati dovranno essere predisposti anche alla luce degli orientamenti forniti dalle autorità, alle quali è assegnato il compito di accreditare gli organismi di certificazione, e dunque di svolgere il ruolo di certificatore in prima persona. In quest'ottica, gli interessati potranno

trattamenti particolarmente problematici enumerati all'art. 37 del Codice. Successivamente l'Autorità ha adottato provvedimenti di semplificazione e chiarimenti (cfr. a tal proposito doc. *web* nr. 1823225, 993385, 996680) anticipando la scelta della sua definitiva eliminazione in ambito europeo.

[157] L'obbligo era previsto dall'art. 32 *bis* del Codice previgente solo nell'ambito dei servizi di comunicazione elettronica.

valutare rapidamente il livello di protezione dati assicurato dai relativi prodotti, servizi e applicazioni (artt. 42, 43 e 57 del GDPR).

### *4.2 Il principio dello sportello unico (one stop shop)*

Il nuovo Regolamento europeo introduce all'art. 56 il principio dello sportello unico (*one stop shop*). Il principio prevede che il titolare del trattamento può rivolgersi all'Autorità Garante del Paese in cui è stabilito, la quale opererà come autorità capofila (*leading authority*) per tutte le attività svolte in tutti i Paesi dell'Unione Europea. Fortemente auspicato in quanto semplificatore delle procedure, consente alle imprese di scegliersi l'Autorità di vigilanza con la quale avranno a che fare, potendo decidere dove stabilire la sede nell'ambito del territorio dell'Unione[158]. Al fine di assicurare un'applicazione coerente in tutta l'Unione Europea, il Regolamento prevede il meccanismo di coerenza per la cooperazione tra le Autorità di controllo. Il procedimento si applica quando un'Autorità di controllo intenda adottare una misura intesa a produrre effetti giuridici con riguardo ad attività di

[158] Il concetto di «stabilimento principale» (art. 4, paragrafo 1, punto 16) forma sistema con quanto previsto dall'art. 56, paragrafo 1, in riferimento all'Autorità di controllo capofila, individuata in quella dello Stato in cui il titolare o il responsabile del trattamento ha lo stabilimento principale (o lo stabilimento unico). Nel caso in cui il titolare o il responsabile del trattamento abbiano stabilimenti in più Stati, è chiaro che spetta all'Autorità capofila esercitare il controllo sui trattamenti operati in più Stati dell'Unione Europea, e dunque oltre le frontiere dello Stato in cui ha sede lo stabilimento principale. Il concetto di stabilimento principale non è però direttamente connesso con il tema del trasferimento dei dati all'estero inteso come in Paesi terzi rispetto alla UE.

trattamento che incidono in maniera sostanziale su un numero significativo di interessati in vari Stati membri. Il meccanismo di coerenza vede protagonista il Comitato europeo per la protezione dei dati, che uniforma l'interpretazione e l'applicazione del Regolamento[159].

### *4.3 Garante europeo della protezione dei dati*

Il Garante europeo della protezione dei dati (GEPD) è un'autorità di sorveglianza indipendente il cui obiettivo primario è garantire che le istituzioni e gli organi dell'UE rispettino il diritto alla vita privata e alla protezione dei dati in sede di trattamento dei dati personali e di elaborazione di nuove politiche. Il Regolamento (UE) 2018/1725 definisce i doveri e i poteri del Garante europeo della protezione dei dati (capo IV), nonché l'indipendenza istituzionale del GEPD in qualità di autorità di controllo. Definisce altresì le norme relative alla protezione dei dati nelle istituzioni dell'UE. Le attività del GEPD possono essere suddivise in tre ruoli principali: supervisione, consultazione e cooperazione[160].

---

[159] Sul c.d. *one-stop-shop* e il connesso meccanismo di coerenza di cui all'attuale art. 63 del Regolamento UE 2016/679, cfr. *Working Party article 29, Statement of the Working Party on current discussion in the Council regarding the EU General Data Protection Regulation*, *Main points for one-stop-shop and consistency mechanism for business and individuals*, 16 aprile 2014.

[160] Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio del 23 ottobre 2018 sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE ha istituito il Garante europeo della protezione dei dati (GEPD). Il GEPD è un organismo indipendente dell'UE responsabile del monitoraggio dell'applicazione delle norme sulla protezione dei dati

### *4.4 Il Comitato europeo per la protezione dei dati*

Dal 25 maggio 2018 il Gruppo di lavoro Articolo 29 ha cessato la sua attività ed è stato sostituito dal Comitato Europeo per la Protezione dei Dati (*European Data Protection Board* – EDPB). L'art. 68 del Regolamento istituisce il Comitato europeo per la protezione dei dati come organismo indipendente dell'Unione, dotato di personalità giuridica. È un organismo che definisce le linee comuni di applicazione della disciplina europea uniforme[161]. Rappresentato dal suo Presidente (art. 69), è composto dalle figure di vertice delle Autorità di controllo degli Stati membri e, con diritto di voto limitato, dal Garante Europeo. Ai sensi dell'art. 75, il Comitato si avvale di una segreteria che ha il compito di supportarlo nelle sue attività. La Commissione Europea ha diritto di partecipare ai suoi lavori senza diritto di voto. Compiti e poteri del Comitato sono definiti dall'art. 70, la norma cardine di tutto il sistema, sulla base di un elenco che va dalla lettera a) fino alla lettera y). Le funzioni svolte sono le seguenti: a) sorveglia il Regolamento e ne assicura l'applicazione corretta; b) fornisce consulenza alla

nell'ambito delle istituzioni europee e dell'istruzione dei reclami. Il Regolamento (UE) 2018/1725 stabilisce le norme applicabili al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione europea. È in linea con il regolamento generale sulla protezione dei dati e con la direttiva sulle attività di contrasto in materia di protezione dei dati. È entrato in vigore l'11 dicembre 2018.

[161] BIASIOTTI A. (2018), *Il nuovo regolamento europeo sulla protezione dei dati. Una guida pratica alla nuova privacy e ai principali adempimenti del Regolamento UE 2016/679, aggiornata al D.lgs. 101/2018*, EPC Editore, Roma, IV edizione, p. 259 ss.; ZAMBRANO V. (2019), *Il Comitato europeo per la protezione dati*, in CUFFARO V., D'ORAZIO R., RICCIUTO V. (a cura di), *I dati personali nel diritto europeo*, G. Giappichelli Editore, Torino, p. 985 ss.

Commissione; c) pubblica linee guida, raccomandazioni e migliori prassi; d) elabora per le Autorità di controllo linee guida riguardanti l'applicazione delle misure correttive e la fissazione delle sanzioni amministrative pecuniarie; e) effettua l'accreditamento di organismi di certificazione; f) emette pareri sui progetti di decisione delle Autorità di controllo conformemente al meccanismo di coerenza; g) emette pareri sui codici di condotta redatti a livello di Unione. Il compito essenziale che più caratterizza il ruolo di questo organo è quello indicato dalla lettera a): «sorveglia il Regolamento e ne assicura l'applicazione corretta nei casi previsti dagli artt. 64 e 65, fatti salvi i compiti delle Autorità nazionali di controllo». Dunque, il Comitato ha un compito generale di sorveglianza: supervisiona l'attuazione del Regolamento e vigila sulle Autorità nazionali, nel rispetto dei loro specifici compiti.

## 5. Le direttive gemelle: novità sui contenuti e servizi digitali e sui contratti di vendita ai consumatori

Il commercio elettronico è un motore di crescita chiave del mercato interno europeo. I dati e le informazioni sulle persone fisiche sono diventati nel corso degli anni dei beni equiparabili al denaro e addirittura definiti "nuovo petrolio"[162]. Il 22 maggio 2019 sono state pubblicate nella Gazzetta Ufficiale dell'Unione Europea due nuove

[162] «L'enorme massa di dati personali che ogni giorno gli utenti riversano in rete è il nuovo petrolio, il motore della nuova economia». A parlare è KEEN A., imprenditore e scrittore angloamericano noto in rete per le sue posizioni critiche nei confronti del *web* 2.0, intervenuto dal palco della *Next Conferenc*e 2011 di Berlino. Secondo l'autore, siamo in un nuovo «*wild west* tecnologico», dove la nostra *privacy* – e con essa le nostre vite – è in vendita al miglior offerente.

direttive del Parlamento Europeo volte ad unificare la disciplina della vendita di beni e della fornitura di contenuto digitale e servizi digitali[163]: 1. Direttiva (UE) 770/2019 relativa a determinati aspetti dei contratti di fornitura di contenuti digitali e di servizi digitali[164]; 2. Direttiva (UE) 771/2019 relativa a determinati aspetti dei contratti di vendita di beni[165]. Le direttive si fondano sul principio della "massima armonizzazione", in virtù del quale gli Stati membri non possono discostarsi dalle prescrizioni ivi previste, ad eccezione di taluni aspetti. Gli Stati membri, che potranno mantenere o introdurre norme nazionali più rigorose per proteggere i consumatori, avranno tempo fino al 1° luglio 2021 per adottare le misure necessarie per conformarsi alle nuove direttive che saranno quindi applicabili dal 1° gennaio 2022. Tali norme hanno natura imperativa, pertanto, non appena la direttiva sarà attuata nella legislazione nazionale, le imprese che vendono ai consumatori dovranno adeguare i propri testi contrattuali (ad es. le condizioni generali di vendita) alle nuove disposizioni. A partire dal 1° gennaio 2022, la

[163] In dottrina si veda CAMARDI C. (2019), *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali*, Giustizia Civile, 3, p. 499; STAZI A. (2019), *Automazione contrattuale e "contratti intelligenti". Gli smart contracts nel diritto contrattuale comparato*, G. Giappichelli Editore, Torino, p. 35 ss.

[164] Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali. Disponibile *online* al seguente indirizzo *world wide web*: https://eur-lex.europa.eu/legal-content/IT/TXT/?qid=1578578066418&uri=CELEX:32019L0770.

[165] Direttiva (UE) 2019/771 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di vendita di beni, che modifica il regolamento (UE) 2017/2394 e la direttiva 2009/22/CE, e che abroga la direttiva 1999/44/CE. Disponibile *online*: https://eur-lex.europa.eu/eli/dir/2019/771/oj.

direttiva 1999/44/CE[166], relativa a vendite di beni di consumo e garanzie associate a tali vendite verrà abrogata per fare spazio alla nuova direttiva UE n. 771 adottata il 20 maggio 2019. Le disposizioni della Direttiva 1999/44/CE sono state recepite da tempo in Italia e sono ora contenute negli articoli da 129 a 134 del decreto legislativo n. 206 del 6.9.2005 (Codice del Consumo)[167]. Entrambe le direttive si inseriscono nell'obiettivo, a livello europeo, di instaurare un mercato unico digitale e garantire lo sviluppo del commercio elettronico e delle attività transfrontaliere verso le vendite al consumo di beni, da un lato, e armonizzare il livello di protezione dei consumatori all'interno dell'Unione Europea, aumentando la certezza giuridica relativamente ai contratti di vendita, dall'altro[168]. Nel perseguire tali obiettivi, alcune previsioni della precedente direttiva rimangono tuttavia invariate[169]. Tra queste: la

[166] Direttiva 1999/44/CE del Parlamento europeo e del Consiglio, del 25 maggio 1999, su taluni aspetti della vendita e delle garanzie dei beni di consumo Gazzetta ufficiale n. L 171 del 07/07/1999 pag. 0012 – 0016. Disponibile *online* al seguente indirizzo *web*: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:31999L0044.

[167] Il CODICE DEL CONSUMO è una norma della Repubblica italiana in materia di diritti del consumatore, emanata con il decreto legislativo 6 settembre 2005, n. 206. Disponibile *online* al seguente indirizzo *web*: https://www.agcm.it/competenze/tutela-del-consumatore/pratiche-commerciali-scorrette/dettaglio?id=e020532b-9cea-46b8-b8f7-27a788825dd0.

[168] RINALDI G.M., BRESCHI M. (BIRD & BIRD LLP) (2020), *Le direttive "gemelle"*. Disponibile *online* al seguente indirizzo *world wide web*: https://www.twobirds.com/~/media/pdfs/italy/bird-bird-le-direttive-gemelle-novita-sui-contenuti-e-servizi-digitali-e-sui-contratti.pdf?la=it&hash=E43E6C32B2A9933E47114F3AB0518FC74C719D92. Data di ultima consultazione: 17 giugno 2021.

[169] MANTELLI DAVINI AVVOCATI ASSOCIATI INTERNATIONAL CONTRACT LAWYERS (2021), *Novità in tema di tutela e garanzie legali e commerciali dei consumatori: la nuova Direttiva UE 2019/771.* Disponibile *online* al seguente indirizzo *web*: https://imantelli.eu/novita-in-tema-di-tutela-

responsabilità del venditore nei confronti del consumatore per qualsiasi difetto di conformità sussistente al momento della consegna del bene e che si manifesta entro due anni da tale momento a durata della garanzia (sempre due anni); i requisiti per la conformità dei beni oggetto del contratto di vendita; i diritti del consumatore, in caso di difetto di conformità, alla riparazione o alla sostituzione del bene.

### *5.1 Contratti di fornitura di contenuti e servizi digitali (direttiva UE 770/2019)*

La Direttiva (UE) 770/2019 fa parte della strategia per il mercato unico digitale in Europa[170] e stabilisce norme relative ai contratti per la fornitura di contenuti digitali o servizi digitali, in particolare: regole di conformità al contratto; e i rimedi in caso di difetto di conformità o di mancata fornitura dei contenuti digitali o dei servizi digitali. I contenuti digitali comprendono programmi informatici, applicazioni, *file* video e audio in formato digitale. I servizi digitali comprendono, ad esempio, i

e-garanzie-legali-e-commerciali-dei-consumatori-la-nuova-direttiva-ue-2019-771/. Data di ultima consultazione: 17 giugno 2021.

[170] NUOVA STRATEGIA PER IL MERCATO UNICO DIGITALE IN EUROPA. Un mercato unico digitale consentirebbe ai consumatori e alle imprese di beneficiare pienamente delle opportunità offerte dalle tecnologie digitali e di *Internet*. La strategia definisce 16 azioni mirate basate su tre pilastri: 1. Un migliore accesso per i consumatori ai beni e servizi digitali in tutta Europa; 2. Creare un contesto favorevole e parità di condizioni per lo sviluppo di reti digitali e servizi innovativi; 3. Massimizzare il potenziale di crescita dell'economia digitale. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni «Strategia per il mercato unico digitale in Europa», COM(2015) 192 *final* del 6.5.2015. Disponibile *online*: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=LEGISSUM:3102_3.

servizi di *cloud computing* e i *social media*. La direttiva si applica a qualsiasi contratto di fornitura di un contenuto/servizio digitale[171] al consumatore (anche in caso di customizzazione), dietro il pagamento di un prezzo o il trasferimento di dati personali del consumatore medesimo al fornitore, sempre che quest'ultimo tratti tali dati esclusivamente ai fini della fornitura del contenuto/servizio digitale a norma della direttiva o per l'assolvimento degli obblighi di legge e il fornitore non tratti tali dati per scopi diversi da quelli previsti. La direttiva stabilisce norme relative alla conformità del contenuto/servizio digitale al contratto di fornitura; ai rimedi in caso di difetto di conformità al contratto o in caso di mancata fornitura e alle modalità di esercizio degli stessi; alla modifica del contenuto/servizio digitale. Gli operatori economici assicurano che il consumatore venga informato e riceva gli aggiornamenti, anche di sicurezza, necessari a mantenere la conformità del contenuto digitale o del servizio digitale. La direttiva contiene inoltre disposizioni dettagliare sull'obbligo di fornire

[171] Ai sensi dell'art. 2, n. 2, della Direttiva 770/2019, per "contenuto digitale" si intende i dati e i prodotti forniti in formato digitale. Data l'ampiezza della definizione, vi possono rientrare programmi informatici, applicazioni, *file* video, *file* audio, *file* musicali, giochi digitali, libri elettronici o altre pubblicazioni elettroniche nonché qualunque materiale, documento, *file* in formato digitale. Per "servizio digitale" si intende i) un servizio che consente al consumatore di creare, trasformare, archiviare i dati o di accedervi in formato digitale, oppure ii) un servizio che consente la condivisione di dati in formato digitale caricati o creati dal consumatore e da altri utenti di tale servizio o qualsiasi altra interazione con tali dati. Sono inclusi, perciò, tutti i servizi di *cloud computing* forniti ai consumatori (quali, per esempio, i servizi Saas, Paas, Iaas) nonché quelli per la condivisione audio e video e altri tipi di *file hosting*, la videoscrittura o i giochi *online* offerti anche tramite *social media* o altre piattaforme. Cfr. RINALDI G.M., BRESCHI M. (BIRD & BIRD LLP) (2020), op. cit.

aggiornamenti. Ai sensi della direttiva, il fornitore ha adempiuto l'obbligo di fornitura quando il contenuto/servizio digitale o qualunque mezzo idoneo per accedere o scaricare il contenuto digitale è reso disponibile o accessibile al consumatore. La grande novità della Direttiva 2019/770 è che essa conferisce espressamente al consumatore l'opportunità di vedersi riconosciuta la possibilità di attivare i rimedi contrattuali anche laddove abbia pagato trasferendo i propri dati personali, essendo ormai data per assunta la natura di corrispettivo contrattuale degli stessi. Il consumatore potrà azionare i rimedi previsti in caso di mancata fornitura ovvero di difetto di conformità del servizio o del contenuto digitale[172].

### *5.2 Contratti di vendita di beni (direttiva UE 771/2019)*

La Direttiva (UE) 771/2019 prevede l'introduzione di nuove norme concernenti i contratti di vendita conclusi tra venditori e consumatori, in particolare con riferimento: alla conformità dei beni al contratto; ai rimedi in caso di difetto di conformità e sulle modalità di esercizio degli stessi; alle garanzie commerciali. La direttiva contiene disposizioni parallele a quelle previste dalla direttiva 770/2019. Ai sensi dell'art. 3, la direttiva 771/2019 si applica ai contenuti digitali o ai servizi incorporati o interconnessi con beni e che sono forniti con il bene ai sensi del contratto di vendita,

[172] DELLI PONTI A., LENZI E. – STUDIO LEGALE STEFANELLI (2019), *Mercato unico digitale: la nuova normativa per la fornitura di servizi online dell'UE*. Articolo disponibile al seguente indirizzo *world wide web*: https://www.studiolegalestefanelli.it/it/approfondimenti/mercato-unico-digitale-nuova-normativa-per-fornitura-di-servizi-online-ue/#_ftn2. Data di ultimo accesso e consultazione: 20 giugno 2021.

indipendentemente dal fatto che detti contenuti o servizi digitali siano forniti dal venditore o da terzi[173]. In altri termini, la direttiva si applica solo ai contratti di vendita tra un consumatore e un venditore (B2C) relativi a beni mobili materiali e si applica sia alla vendita *online* che a quella *offline*. Tema specifico della direttiva è invece quello relativo alla garanzia commerciale, la quale deve integrare tutti i requisiti introdotti dalla direttiva e deve essere consegnata al più tardi al momento della consegna dei beni. Inoltre, se le condizioni stabilite nella garanzia commerciale sono meno vantaggiose per il consumatore rispetto a quelle stabilite nella relativa pubblicità, la garanzia commerciale vincola secondo le condizioni stabilite nella pubblicità, a meno che quest'ultima sia stata corretta secondo le stesse modalità o con modalità simili a quelle in cui è stata resa, prima della conclusione del contratto. Tre le principali novità introdotte dalla Direttiva 2019/771 relativa a taluni aspetti della vendita e delle garanzie dei beni di consumo modernizzandone e armonizzandone alcuni aspetti, vi sono[174]: la responsabilità del venditore per qualsiasi difetto di conformità sussistente al momento della consegna del bene e che si manifesta entro due anni da tale momento; sono compresi i beni con contenuto digitale ed i beni il cui contenuto digitale venga

[173] IPSOA REDAZIONE (2019), *Contratti di vendita di beni e di contenuto digitale: l'UE adotta nuove norme*. Disponibile *online* al seguente indirizzo *Internet*: http://www.ipsoa.it/documents/impresa/contratti-dimpresa/quotidiano/2019/04/16/contratti-vendita-beni-contenuto-digitale-ue-adotta-nuove-norme. Ultimo acceso: 18 giugno 2021.

[174] STUDIO LEGALE STEFANELLI (2019), *Mercato unico digitale: la nuova normativa per la fornitura di servizi online dell'UE*. Articolo disponibile *online* al seguente indirizzo *world wide web* per la consultazione: https://www.studiolegalestefanelli.it/it/approfondimenti/mercato-unico-digitale-nuova-normativa-per-fornitura-di-servizi-online-ue/#_ftn2. Data di ultima consultazione e accesso: 20 giugno 2021.

fornito in maniera continuativa per un periodo di tempo previsto contrattualmente; la Direttiva stabilisce nel dettaglio i requisiti soggettivi (art. 6) e oggettivi (art. 7) di conformità che il bene deve rispettare; l'inversione dell'onere della prova, per cui qualsiasi difetto di conformità che si manifesta entro un anno dal momento della consegna si presume come già esistente al momento della consegna (con possibilità per gli Stati membri di allungare il periodo fino a 2 anni); in caso di difetto di conformità il consumatore ha diritto al ripristino della conformità del bene, alla riduzione del prezzo o alla risoluzione del contratto.

## 6. Il nuovo approccio europeo all'intelligenza artificiale

"L'intelligenza artificiale (IA) non è fantascienza: fa già parte delle nostre vite. Che si tratti di utilizzare un assistente personale virtuale per organizzare la nostra giornata lavorativa, viaggiare in un veicolo a guida autonoma o avere un telefono che ci suggerisce le canzoni o i ristoranti che potrebbero piacerci, l'IA è una realtà"[175]. Per far in modo che vengano usate tecnologie basate sull'intelligenza artificiale è necessario il libero flusso di dati all'interno dell'Unione Europea e occorre garantire un forte livello di sicurezza, riservatezza e protezione dei dati; da questi contrasti nascono una serie di questioni legali ed etiche nella ricerca di un equilibrio tra i notevoli progressi sociali e tecnologici in nome dell'intelligenza artificiale e i diritti fondamentali in tema

[175] Commissione europea nella Comunicazione al Parlamento europeo, al Consiglio europeo, al Comitato economico e sociale europeo e al Comitato europeo delle regioni, *L'intelligenza artificiale per l'Europa,* COM(2018) 237 *final*. Bruxelles, 25 aprile 2018, p. 1.

di *privacy*. Durante la plenaria del 20 ottobre 2020[176], il Parlamento Europeo[177] ha approvato due iniziative legislative e una relazione[178] in cui affronta diversi temi legati all'uso dell'IA. Nella prima iniziativa legislativa si sollecita la Commissione UE a presentare un nuovo quadro giuridico che delinei i principi etici e gli obblighi legali da seguire nello sviluppo, nell'implementazione e nell'utilizzo dell'intelligenza artificiale, della robotica e delle tecnologie correlate nell'UE, compresi *software*, algoritmi e dati. Nell'iniziativa legislativa sugli aspetti etici si sottolinea che le leggi future dovrebbero tenere conto di diversi principi guida. L'IA dovrebbe essere incentrata sull'uomo. Inoltre, gli altri principi dovrebbero riguardare la sicurezza, la trasparenza, la responsabilità, la salvaguardia contro i pregiudizi e le discriminazioni, il diritto al risarcimento, la responsabilità sociale e ambientale e il rispetto dei diritti fondamentali. Nella seconda iniziativa legislativa, invece, gli eurodeputati richiedono un quadro giuridico in materia

[176] Parlamento Europeo (2020), *Intelligenza artificiale: Il PE getta le basi per le prime regole UE*. Disponibile *online* al seguente indirizzo: https://www.europarl.europa.eu/news/it/agenda/briefing/2020-10-19/2/intelligenza-artificiale-il-pe-getta-le-basi-per-le-prime-regole-ue.

[177] Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate (2020/2012(INL)), disponibile *online*: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_IT.html. Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL)), disponibile: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_IT.html#title3.

[178] Risoluzione del Parlamento europeo del 20 ottobre 2020 sui diritti di proprietà intellettuale per lo sviluppo di tecnologie di intelligenza artificiale (2020/2015(INI)), disponibile *online* al seguente indirizzo *web*: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_IT.html.

di responsabilità civile orientato al futuro, che renda gli operatori IA ad alto rischio oggettivamente responsabili dei danni che ne possono derivare. Le norme dovrebbero riguardare la protezione della vita, della salute, dell'integrità fisica, della proprietà e dei beni, nonché i danni significativi non materiali, qualora si registri una perdita economica verificabile. Nella relazione, infine, l'Europarlamento chiarisce che la *leadership* globale dell'UE in materia di IA richiede un sistema efficace di diritti di proprietà intellettuale e salvaguardie per far sì che il sistema europeo dei brevetti protegga gli sviluppatori innovativi. Tale sistema dovrebbe occuparsi della personalità giuridica, del diritto d'autore, dei segreti commerciali e della protezione delle opere creative che utilizzino o siano generate dall'IA. Il 21 ottobre 2020 il Consiglio UE ha adottato le sue conclusioni sull'IA e la Carta dei diritti fondamentali, sottolineando che lo sviluppo e l'applicazione dell'intelligenza artificiale devono andare di pari passo con il rispetto di tali diritti, sulla base di un approccio umano-centrico. Dignità, libertà ed uguaglianza sono i principi guida che l'Unione e gli Stati membri devono tenere a mente al fine di delineare il nuovo quadro UE sull'IA, tutelando i diritti dei cittadini in ogni ambito. Il 21 aprile 2021 la Commissione Europea ha presentato un pacchetto di misure[179] che delinea la strategia europea sull'intelligenza artificiale. Per entrare in vigore, il nuovo regolamento dovrà essere discusso e votato dal Parlamento Europeo e dagli Stati membri, processo che

[179] Commissione Europea, COM (2021) 206 del 21.04.2021. *Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*. Disponibile *online* al seguente indirizzo *world wide web*: https://www.europeansources.info/record/proposal-for-a-regulation-laying-down-harmonised-rules-on-artificial-intelligence-artificial-intelligence-act-and-amending-certain-union-legislative-acts/.

richiederà alcuni anni per essere completato[180]. L'iniziativa della Commissione copre diversi ambiti e applicazioni della AI, dai sistemi per le nuove assunzioni di personale nelle aziende agli algoritmi che fanno funzionare le automobili a guida autonoma, passando per il riconoscimento facciale da parte delle forze dell'ordine. In generale, nella proposta di regolamento si prevedono regole di trasparenza armonizzate applicabili a tutti i sistemi di IA, mentre sono previste specifiche disposizioni per i sistemi di IA classificati "ad alto rischio", per i quali viene introdotta una specifica definizione, affinché rispettino determinati requisiti obbligatori relativi alla loro affidabilità. Il regolamento stabilisce che cosa si può e che cosa non è consentito fare con le AI e prevede multe fino al 6 per cento del fatturato annuo delle aziende coinvolte, con meccanismi simili a quelli impiegati per il GDPR. Il nuovo approccio europeo comprende anche una proposta di regolamento sulle macchine, che stabilisce i requisiti di sicurezza dei prodotti, sostituendo l'attuale "Direttiva Macchine"[181]. Il nuovo approccio europeo per l'utilizzo della AI fa seguito ad una serie di iniziative intraprese negli ultimi anni[182], tra cui: la consultazione pubblica sul Libro Bianco sull'Intelligenza Artificiale (COM 2020) 65 *final*

---

[180] IL POST (2021), *Come l'Europa vuole regolamentare le intelligenze artificiali La Commissione Europea ha presentato una proposta molto articolata e ambiziosa sulle tecnologie al centro del nostro futuro*. Disponibile *online*: https://www.ilpost.it/2021/04/22/commissione-europea-intelligenza-artificiale/.

[181] Direttiva 2006/42/CE del Parlamento europeo e del Consiglio, del 17 maggio 2006, relativa alle macchine e che modifica la direttiva 95/16/CE (rifusione). Disponibile *online* al seguente *link*: https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=celex%3A32006L0042.

[182] CAMERA DEI DEPUTATI (2021), *Documentazione Parlamentare*, *Il nuovo approccio europeo all'Intelligenza Artificiale*. Disponibile *online*: https://temi.camera.it/leg18/post/OCD15_14416/il-nuovo-approccio-europeo-all-intelligenza-artificiale.html.

del 19 febbraio 2020[183]; le Linee guida etiche finali per un'intelligenza artificiale affidabile, del Gruppo ad alto livello sull'intelligenza artificiale, pubblicate l'8 aprile 2019; il Rapporto sulla responsabilità per l'Intelligenza Artificiale e altre tecnologie emergenti, del Gruppo di esperti sulla responsabilità e le nuove tecnologie, pubblicato il 21 novembre 2019; la Dichiarazione di cooperazione sull'intelligenza artificiale, firmata da 25 Paesi europei il 10 aprile 2018, che si basa sui risultati e sugli investimenti della comunità europea della ricerca e delle imprese nell'IA e stabilisce le basi per il Piano coordinato sull'IA.

## 7. Nuovi fenomeni lesivi della riservatezza e problemi di tutela del diritto alla protezione dei dati personali

Il diritto alla riservatezza – cioè la pretesa *erga omnes* dell'individuo a mantenere una propria sfera intima intangibile da ingerenze altrui che non siano giustificate da interessi superiori – nel corso del tempo si è trasfuso nel più ampio diritto alla protezione dei dati personali, vale a dire nel diritto a vedere trattati tali dati secondo criteri di liceità e correttezza, sulla base del consenso dell'interessato (o di altro presupposto equipollente), al fine – secondo il cosiddetto principio di autodeterminazione informativa – di poter sempre

[183] Cfr. LIBRO BIANCO sull'intelligenza artificiale – *Un approccio europeo all'eccellenza e alla fiducia*, 19 febbraio 2020, disponibile *online* in web: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_it.pdf. Bruxelles, 19.2.2020 COM(2020) 65 *final*.

mantenere il controllo sul patrimonio delle informazioni che riguardano e identificano l'individuo medesimo[184]. Difatti, le principali linee di sviluppo della normativa concernente i dati personali avviate dagli organi della Unione Europea in fasi progressive sono almeno tre[185]: (a) la prima concerne la protezione dei dati come espressione ed immagine della persona, con specificazione del diritto generale della personalità; (b) un'altra concerne la costruzione del mercato dei dati che sono componente essenziale del mercato digitale, la loro circolazione e il loro trattamento; (c) un'altra ancora attiene ai contratti che hanno contenuto digitale, tra i quali possono essere rinvenuti dati di natura personale. Sono presenti poi altre linee di sviluppo intrecciate con l'informatica, la cibernetica e l'intelligenza artificiale. L'evoluzione del diritto alla *privacy* si riflette così sul Garante per la protezione dei dati personali che, nell'esercizio delle sue funzioni a garanzia di un diritto a rilevanza costituzionale, finisce per regolare progressivamente anche l'attività degli operatori economici (in particolar modo sul *web*) e vigilare un settore di mercato estremamente sensibile a tutela degli utenti[186].

---

[184] BUSIA G. (2019), *Il ruolo dell'autorità indipendente per la protezione dei dati personali*, in ZORZI GALGANO N. (a cura di), *Persona e mercato dei dati. Riflessione sul GDPR,* Cedam, Padova, p. 350.

[185] ALPA G. (2019), *La "proprietà" dei dati personali*, in ZORZI GALGANO N. (a cura di), op. ult. cit., p. 11 ss.

[186] BUSIA G. (2019), *Il ruolo dell'autorità indipendente per la protezione dei dati personali*, in ZORZI GALGANO N. (a cura di), op. ult. cit., p. 355.

### *7.1 Profilazioni e processi decisionali automatizzati*

I progressi nella tecnologia dell'informazione e della comunicazione (in lingua inglese *information and communication technology* – ICT) hanno impresso una forte accelerazione ad attività di *big data analytics*[187] e *data mining*[188], che a loro volta alimentano forme nuove di intelligenza artificiale: (a) *machine learning supervised*, nelle quali gli algoritmi sono stati programmati in modo da raggiungere determinati risultati, e (b) *machine learning unsupervised*, nelle quali gli algoritmi riescono a trovare delle regolarità nell'insieme dei dati, senza alcuna istruzione rispetto ai risultati che devono essere ottenuti[189].

---

[187] Cfr. BAROCAS S., SELBST A.D. (2016), *Big Data's Disparate Impact*, 104 California Law Review, 673: "*Big Data is the buzzword of the decade*". Il termine *big data* (megadati) si riferisce a grandi quantità di tipi diversi di dati prodotti da varie fonti, fra cui persone, macchine e sensori. Alcuni esempi sono i dati sul clima, le immagini satellitari, le immagini e i video digitali, le registrazioni di operazioni o i segnali GPS. I *big data* possono comprendere dati personali: ad es. informazioni riguardanti una persona, come un nome, una fotografia, un indirizzo e-mail, estremi bancari, messaggi postati sui siti delle reti sociali, informazioni cliniche o l'indirizzo IP di un computer: cfr. COMMISSIONE EUROPEA, *Digital single market-Big Data*, disponibile *online* al seguente indirizzo *web*: *ec.europa.eu*.

[188] Si intende per *data mining* il processo di estrazione da banche dati di grandi dimensioni tramite l'applicazione di algoritmi che individuano le associazioni nascoste tra le informazioni e le rendono visibili. L'estrazione di conoscenza avviene tramite l'individuazione delle associazioni o sequenze ripetute (patterns). V. FAYYAD U.M., PIATETSKY-SHAPIRO G., SMYTH P. (1996), *From data mining to knowledge discovery: an overview*, in FAYYAD U.M., *Advances in Knowledge Discovery and Data Mining*, AAAI Press, Menlo Park, CA.

[189] ANGELINI R. (2018), *Intelligenza Artificiale e governance. Alcune riflessioni di sistema*, in PIZZETTI F. (a cura di), *Intelligenza artificiale,*

L'ampia disponibilità di dati personali che popolano la infosfera[190], generati sia da utenti ormai iperconnessi che agiscono come "agenti informazionali o *inforg*"[191] (in un contesto che è stato definito *onlife* per indicare l'erosione della frontiera tra reale e virtuale e il superamento della contrapposizione tra *off line* e *on line*), sia da dispositivi che dialogano tra loro attraverso flussi di informazioni (IOT- *Internet of things*)[192], ha reso concreta in numerosi

*protezione dei dati personali e regolazione*, G. Giappichelli Editore, Torino, p. 295.

[190] FLORIDI L. (2017), *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, Milano, 2017, p. 44 ss.: "a un livello minimo, l'infosfera indica l'intero ambiente informazionale costituito da tutti gli enti informazionali, le loro proprietà, interazioni, processi e reciproche relazioni (…). A un livello massimo, l'infosfera è concetto che può essere utilizzato anche come sinonimo di realtà, laddove interpretiamo quest'ultima in termini informazionali. (…) La transizione dall'analogico al digitale e la crescita esponenziale di spazi informazionali in cui trascorriamo sempre più tempo illustrano con massima evidenza il modo in cui le ICT stanno trasformando il mondo in una infosfera".

[191] *Ivi, op. cit.*, p. 107 ss., a proposito della "quarta rivoluzione" in corso chiarisce che essa non deve essere confusa con l'idea di un'umanità *cyborg*, né con scenari post-umani: piuttosto, le nostre capacità di valutazione e classificazione sono sfruttate per migliorare le *performance* di alcune tecnologie dell'informazione e della comunicazione. V. anche FLORIDI L. (2009), *Infosfera. Etica e filosofia nell'età dell'informazione*, G. Giappichelli Editore, Torino, p. 185 ss.

[192] INTERNET SOCIETY (2015), *The Internet of Things: An Overview*, definisce la IOT come la capacità di oggetti, dispositivi, sensori ed altri oggetti che normalmente non sono considerati computer, di alloggiare capacità elaborativa di connettersi alla rete *internet*. Questi oggetti intelligenti possono generare, scambiare, utilizzare dati richiedendo un intervento umano minimo e possono connettersi a sistemi remoti per la raccolta e analisi dei dati o per la loro gestione. Qualche esempio: dispositivi indossabili (come gli *activity tracker*), sistemi domotici (come gli elettrodomestici intelligenti), sistemi per *smart cities* e *connected*

contesti la possibilità di analizzare e prevedere modelli di comportamento, abitudini, interessi. Tecniche di profilazione e decisioni (totalmente o parzialmente) automatizzate sono ampiamente utilizzate in una molteplicità di ambiti, sia pubblici che privati: es. sanità, *marketing*, concessione del credito, assicurazione, tassazione[193]. I recenti sviluppi di nuove forme di intelligenza artificiale collegate alle profilazioni e ai processi decisionali automatizzati hanno aperto nuovi dibattiti nella letteratura giuridica[194]. Il GDPR ha rafforzato il complesso delle tutele soggettive, attribuendo all'individuo poteri di controllo più incisivi sui processi di trattamento dei dati personali e ponendo in capo al titolare

*car*. Sui rischi della tecnologia IOT v. BENEDETTI D., *IA e (in)sicurezza informatica*, in PIZZETTI F. (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, cit., p. 243 ss.

[193] PELLECCHIA E. (2018), *Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation*, Le nuove leggi civili commentate, 41(5), 1209 – 1235.

[194] Sul tema delle profilazioni e decisioni automatizzate cfr. l'attenta riflessione di MESSINETTI R. (2019), *Trattamento dei dati per finalità di profilazione e decisioni automatizzate*, in ZORZI GALGANO N. (a cura di), op. cit., pp. 167 – 193. La letteratura scientifica ne sta discutendo da tempo risalente, provando a immaginare quali effetti sull'individuo e sulla società possano conseguire ad un uso sistemico e generalizzato di simili strumenti statistici. Cfr. RODOTÀ S. (1995), *Tecnologie e diritti*, Il Mulino, Bologna; ID. (2004), *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza Editore, Roma-Bari, p. 164 ss.; ID. (2012), *Il diritto di avere diritti*, Laterza Editore, Roma-Bari, passim. V. inoltre PELLECCHIA E. (2018), *Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation*, Le nuove leggi civili commentate, 41(5), 1209 – 1235.

del trattamento nuovi doveri[195]. La trasparenza si pone dunque come principio generale e si ritrova alla radice del diritto di essere informato di cui agli artt. 13 e 14 e del diritto di accesso di cui all'art. 15, richiedendo – nelle peculiari ipotesi di profilazione[196] e di processi decisionali automatizzati – che l'individuo sia informato in maniera chiara e semplice anche delle modalità funzionali del trattamento. Nel caso specifico previsto dall'art. 22 (processo decisionale totalmente automatizzato) implica che la relazione comunicativa tra titolare dei dati e titolare del trattamento includa in particolare informazioni significative sulla logica utilizzata nel trattamento, sull'importanza e le conseguenze previste per la persona[197].

---

[195] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, p. 16.

[196] Cfr. art. 4 GDPR – Definizioni, nr. 4: «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica. La profilazione si caratterizza quindi per la concorrente presenza di tre elementi: 1. si deve trattare di una forma automatizzata di elaborazione; 2. deve essere effettuato su dati personali; 3. l'obiettivo deve essere quello di valutare aspetti personali di un soggetto.

[197] Cfr. art. 22 GDPR – Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione: 1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. 2. Il paragrafo 1 non si applica nel caso in cui la decisione: a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato

Il contenuto di queste disposizioni ha acceso un vivace dibattito in letteratura se il GDPR garantisca o meno all'individuo la possibilità di conoscere le ragioni della decisione che costituisca l'*output* finale di un processo automatizzato. Oltre il diritto alla trasparenza, vi è poi il diritto di resistenza della persona al potere decisionale dell'apparato tecnologico; difatti, l'art. 21 riconosce espressamente all'interessato il diritto di opporsi alla profilazione, in qualsiasi momento, per motivi connessi alla sua situazione particolare, nei soli casi in cui il trattamento dei dati rientri nelle previsioni di cui all'art. 6, par. 1, lett. e) e f) del GDPR[198]. Il diritto di opposizione

membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato. 3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione. 4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

[198] Cfr. art. 21 GDPR – Diritto di opposizione: 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

risulta di efficacia conclusiva nel caso del *marketing* diretto (par. 2). In tutte le altre ipotesi, il successo dell'opposizione dell'interessato è subordinato alla non dimostrazione da parte del titolare del trattamento dell'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. La profilazione implica sempre una qualche forma di valutazione o giudizio su una persona: una semplice classificazione di individui in base a caratteristiche note come età, sesso e altezza non conduce necessariamente alla profilazione, dipenderà dallo scopo della classificazione. Il processo decisionale automatizzato ha una portata diversa e può parzialmente sovrapporsi o risultare dalla profilazione, nel senso che decisioni automatizzate possono essere prese con o senza profilazione (e la profilazione può non essere funzionale a decisioni automatizzate) e in maniera

---

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 riguardano, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

parzialmente o totalmente automatizzata[199]. Benefici, in termini di maggiore efficienza delle organizzazioni e risparmio di risorse, e rischi, specialmente con riguardo ai diritti e alle libertà delle persone, devono essere attentamente valutati e bilanciati, soprattutto a fronte della conclamata opacità di molte delle tecniche di profilazione e di decisione automatizzata[200]. La velocità e la portata delle modificazioni della realtà legate agli sviluppi delle tecnologie dell'informazione e della comunicazione non consentono di prevedere se i nuovi strumenti normativi siano idonei a proteggere la persona dai rischi per i suoi diritti e libertà fondamentali, correlati alla nuova vulnerabilità di fronte all'apparato tecnologico e al suo potere digitale[201]. Il punto cruciale del problema è l'identità profilata assunta quale punto di riferimento di decisioni

[199] PELLECCHIA E. (2018), *Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation*, Le nuove leggi civili commentate, 41(5), 1209 – 1235.

[200] Cfr. CERQUITELLI T., QUERCIA D., PASQUALE F. (2017), *Transparent Data Mining for Big and Small Data*, Springer International, New York, passim. Il manuale si concentra su soluzioni nuove ed emergenti di *data mining* che offrono un livello di trasparenza maggiore rispetto alle soluzioni esistenti. In particolare, sono trattate soluzioni di *data mining* trasparenti con proprietà desiderabili (ad esempio efficaci, completamente automatiche, scalabili). I risultati sperimentali di soluzioni trasparenti sono adattati a diversi esperti di dominio; inoltre, vengono presentate metriche sperimentali per valutare la trasparenza algoritmica. Il volume discute anche gli effetti sociali della scatola nera rispetto agli approcci trasparenti al *data mining*, nonché i casi d'uso del mondo reale per questi approcci. Poiché gli algoritmi supportano sempre più aspetti diversi della vita moderna, è assolutamente necessario un maggiore livello di trasparenza, non ultimo perché si devono evitare discriminazioni e pregiudizi.

[201] RODOTÀ S. (2012), *Il diritto di avere diritti*, Laterza Editore, Roma-Bari, p. 335, per approfondimento sulla "nuova vulnerabilità sociale".

prese da altri e capaci di incidere nella vita della persona: assumere decisioni fondate sulla capacità comunicativa del profilo significa decidere sulla persona in base all'insieme delle possibilità valutative e predittive che risultano consentite e rese visibili dalla categoria statistica cui la persona appartiene[202]. In altre parole, profilazione e decisioni automatizzate possono segregare le persone in specifiche categorie riducendo la loro possibilità di scelta, possono consolidare gli stereotipi, scoraggiare azioni rivelatrici di condotte divergenti, produrre discriminazioni inattese[203].

### *7.2 Neuroprivacy*

La *neuroprivacy* – o *privacy* cerebrale – è un concetto che si riferisce ai diritti che le persone hanno riguardo all'*imaging* (o *imaging* biomedico o diagnostica per immagini), all'estrazione e all'analisi dei dati neurali dal loro cervello. Questo concetto è strettamente correlato a campi come la neuroetica, la neurosicurezza e il neurodiritto ed è diventato sempre più rilevante con lo sviluppo e il progresso di varie tecnologie di *neuroimaging*. La *neuroprivacy* è un aspetto della neuroetica che riguarda

---

[202] MESSINETTI R. (2019), *Trattamento dei dati per finalità di profilazione e decisioni automatizzate*, in ZORZI GALGANO N. (a cura di), op. cit., p. 192.

[203] PELLECCHIA E. (2018), op. cit. L'autrice continua sostenendo che "Facebook definisce chi siamo, Amazon cosa vogliamo, Google cosa pensiamo: soprattutto, la nostra reputazione – per lo più ricostruita sulla interpretazione delle tracce che lasciamo nelle nostre interazioni in rete, nonché sulla base di dati disponibili su di noi, anche quando generati da terzi - definisce il nostro orizzonte di opportunità".

specificamente l'uso delle informazioni neurali in casi legali, *neuromarketing*, sorveglianza e altri scopi esterni, nonché le corrispondenti implicazioni sociali ed etiche[204]. Concetti neuroetici come la *neuroprivacy* si sono sviluppati inizialmente negli anni 2000, dopo l'invenzione iniziale e lo sviluppo di tecniche di *neuroimaging* come la tomografia a emissione di positroni (PET), l'elettroencefalografia (EEG) e la risonanza magnetica funzionale (fMRI)[205]. Poiché il *neuroimaging* è diventato altamente studiato e reso popolare negli anni Novanta, ha anche iniziato a entrare nel mercato commerciale poiché gli imprenditori hanno cercato di commercializzare le applicazioni pratiche delle neuroscienze, come il *neuromarketing*, il *neuroenhancement* e la rilevazione della menzogna. La *neuroprivacy* consiste nelle questioni relative alla *privacy* sollevate sia dalla ricerca neuroscientifica che dagli usi applicati delle tecniche di *neuroimaging*. La rilevanza del dibattito sulla *neuroprivacy* è aumentata in modo significativo dopo gli attacchi terroristici dell'11 settembre 2001, il che ha portato a una spinta per una maggiore *neuroimaging* nel contesto del rilevamento e della sorveglianza di informazioni e minacce[206]. I neurodati sono preziosi per le entità

[204] THE COMMITTEE ON SCIENCE AND LAW (2005), *Are Your Thoughts Your Own?: 'Neuroprivacy' and the Legal Implications of Brain Imaging,* The Record of the Association of the Bar of the City of New York, 60(2), pp. 407–437. Disponibile *online* in formato PDF al seguente indirizzo *web*: https://www2.nycbar.org/Publications/record/vol.%2060%20no.%202.pdf.

[205] VIDAL F. (2015), *Historical and Ethical Perspectives of Modern Neuroimaging*, in CLAUSEN J., LEVY N. (eds), *Handbook of Neuroethics*, Springer, Dordrecht.

[206] LITTLEFIELD M. (2008), *Constructing the Organ of Deceit*, Science, Technology, & Human Values, 34 (3), 365–392; MCCORMICK B. (2006),

pubblicitarie e di *marketing* in quanto possono identificare come e perché le persone reagiscono a stimoli diversi al fine di influenzare meglio i consumatori. Questa capacità di esaminare reazioni e percezioni dal cervello crea direttamente nuovi dibattiti etici, come in che modo definire i limiti accettabili della manipolazione mentale e come evitare di prendere di mira i dati demografici vulnerabili/ricettivi[207]. Attualmente manca la comprensione scientifica di ciò che può essere interpretato dai neurodati, il che rende difficile limitare e classificare i diversi tipi di neurodati e quindi complicare la *neuroprivacy*. Un'altra complicazione è che i neurodati sono altamente personali ed essenzialmente inseparabili dal soggetto, il che lo rende estremamente sensibile e difficile da anonimizzare. Un modo possibile per regolare e proteggere la *neuroprivacy* è concentrarsi sui diversi usi e casi dei neurodati[208]. Esistono vari argomenti legali su come la *neuroprivacy* sia coperta dalle attuali protezioni e diritti e su come le future leggi dovrebbero essere implementate per definire e proteggere la *neuroprivacy*, poiché la neuroscienza ha il potenziale per cambiare significativamente lo *status quo* legale[209]. La definizione

---

*Your Thoughts May Deceive You: The Constitutional Implications of Brain Fingerprinting Technology and How it May Be Used to Secure Our Skies*, Law & Psychology Review, 30, 171–184.

[207] MATTHEWS S. (2015), *Neuromarketing: What Is It and Is It a Threat to Privacy?*, in CLAUSEN J., LEVY N. (eds), *Handbook of Neuroethics*, Springer, Dordrecht, pp. 1627 –1645.

[208] HALLINAN D., SCHÜTZ P., FRIEDEWALD M., DE HERT P. (2014), *Neurodata and Neuroprivacy: Data Protection Outdated?*, Surveillance & Society, 12(1), 55-72.

[209] CHURCH D.J. (2012), *Neuroscience in the Courtroom: An International Concern*, William & Mary Law Review, 53(5), pp. 1825–1854.

legale di *neuroprivacy* deve ancora essere adeguatamente stabilita, ma sembra esserci un consenso generale sul fatto che dovrebbe essere stabilito un fondamento legale ed etico per i diritti di *neuroprivacy* prima che il *neuroimaging* diventi ampiamente accettato in tutti i contesti legali, aziendali e di sicurezza[210]. La letteratura sostiene che l'introduzione delle neuroscienze in contesti legali ha alcuni vantaggi. La neuroscienza potrebbe potenzialmente risolvere alcuni problemi esaminando direttamente il cervello, data la fiducia scientifica nelle tecniche di *neuroimaging*. Tuttavia, ciò solleva questioni relative al bilanciamento degli usi legali delle neuroscienze con le protezioni della *neuroprivacy*[211]. Alcune preoccupazioni etiche generali riguardanti la *neuroprivacy* ruotano attorno ai diritti personali e al controllo sulle informazioni personali. Con il miglioramento della tecnologia, è possibile che la raccolta di neurodati senza consenso o conoscenza sarà più facile o più comune in futuro. Un argomento è che la raccolta di neurodati è una violazione sia della proprietà personale che della proprietà intellettuale, poiché la raccolta di neurodati implica la scansione sia del corpo che dell'analisi del pensiero[212].

---

[210] PEARLMAN E. (2015), *The brain as site-specific surveillant performative space*, International Journal of Performance Arts and Digital Media, 11 (2), 219–234.

[211] ROSKIES A.L. (2015), *Mind Reading, Lie Detection, and Privacy*, Handbook of Neuroethics, op. cit., pp. 679–695.

[212] MOORE A.D. (2017), *Privacy, Neuroscience, and Neuro-Surveillance*, Res Publica, 23, pp. 159–177.

## 8. Data privacy e data security nel marketing

La *privacy* dei dati (o la *privacy* delle informazioni) è un ramo della sicurezza dei dati interessato alla corretta gestione dei dati: consenso, avviso e obblighi normativi. Più specificamente, le preoccupazioni pratiche sulla *privacy* dei dati spesso ruotano attorno a: 1. se o come i dati vengono condivisi con terze parti; 2. come vengono raccolti o archiviati legalmente i dati; 3. restrizioni normative come il GDPR, HIPAA[213], GLBA[214] o CCPA[215]. Le organizzazioni comunemente credono che proteggere i dati sensibili dagli *hacker* significhi essere automaticamente conformi alle normative sulla *privacy* dei

[213] L'*Health Insurance Portability and Accountability Act* (HIPAA) del 1996 è una legge federale degli Stati Uniti che stabilisce i requisiti di *privacy* e sicurezza dei dati per le organizzazioni incaricate di salvaguardare i dati sanitari protetti (PHI) dei privati.

[214] Il *Gramm-Leach-Bliley Act* (GLBA), anche conosciuto come *Financial Services Modernization Act of* 1999, è una legge statunitense che ha abrogato le disposizioni del *Glass-Steagall Act* del 1933 che prevedevano la separazione tra attività bancaria tradizionale e *investment banking*, senza alterare le disposizioni che riguardavano la *Federal Deposit Insurance Corporation*. La legge fu proposta al Senato da Phil Gramm e alla Camera Jim Leach e Thomas J. Bliley, Jr. Venne firmata dal presidente Bill Clinton il 12 novembre 1999.

[215] Il *California Consumer Privacy Act* (CCPA) è uno statuto statale inteso a migliorare i diritti alla *privacy* e la protezione dei consumatori per i residenti della California, Stati Uniti. Il disegno di legge è stato approvato dalla legislatura dello stato della California e firmato in legge da Jerry Brown, governatore della California, il 28 giugno 2018, per modificare la parte 4 della divisione 3 del Codice civile della California. Chiamato ufficialmente AB-375, l'atto è stato introdotto da Ed Chau, membro dell'Assemblea dello Stato della California, e dal senatore Robert Hertzberg. Gli emendamenti al CCPA, sotto forma di *Senate Bill* 1121, sono stati approvati il 13 settembre 2018. Ulteriori modifiche sostanziali sono state firmate in legge l'11 ottobre 2019. Il CCPA è entrato in vigore il 1° gennaio 2020.

dati. La sicurezza dei dati e la protezione dei dati sono spesso utilizzate in modo intercambiabile, ma esistono differenze nette: (a) la *data security* protegge i dati digitali, come quelli in un *database*, da forze distruttive e da azioni indesiderate di utenti non autorizzati, come un attacco informatico o una violazione dei dati; (b) la *data privacy* regola il modo in cui i dati vengono raccolti, condivisi e utilizzati. Si consideri uno scenario in cui si è fatto di tutto per proteggere le informazioni di identificazione personale (PII). I dati sono crittografati, l'accesso è limitato e sono presenti più sistemi di monitoraggio sovrapposti. Tuttavia, se tali PII sono state raccolte senza il consenso appropriato, si vìola la normativa sulla *privacy* dei dati anche se i dati sono al sicuro. Sebbene si possa avere la *data security* senza la *data privacy*, non è possibile avere la *data privacy* senza la *data security*. Il GDPR europeo è probabilmente la normativa sulla *privacy* dei dati più ampia e completa. Sfortunatamente, è anche fonte di confusione: il *New York Times*, nel maggio 2018, lo ha definito un "*big, confusing mess*"[216]. La normativa garantisce ai cittadini una serie di diritti, tra cui il diritto alla portabilità dei dati, che consente alle persone di spostare i propri dati tra le piattaforme, e il diritto di non essere soggetti a decisioni basate sul trattamento automatizzato dei dati, vietando, ad esempio, l'uso di un algoritmo per respingere i candidati per lavori o prestiti. Il problema è che le implicazioni pratiche di queste regole sono incredibilmente complesse. Il GDPR cerca di presentare un compromesso tra i diversi sistemi e valori di molti Stati membri diversi tra loro. Per questo motivo, molti scienziati e gestori di dati che saranno soggetti alla

[216] COOL A. (2018), *Europe's Data Protection Law Is a Big, Confusing Mess*, The New York Times. Disponibile *online* al seguente indirizzo: https://www.nytimes.com/2018/05/15/opinion/gdpr-europe-data-protection.html. Data di ultimo accesso e consultazione: 11 ottobre 2020.

normativa la trovano incomprensibile e dubitano che la conformità assoluta sia addirittura possibile[217]. A volte le aziende non riescono a capire come l'implementazione della protezione dei dati aiuti i loro profitti migliorando la percezione dei clienti della loro reputazione e, a loro volta, guidando più vendite o nuovi affari. Dopotutto, le aziende vengono create per realizzare un profitto e se non esiste una correlazione diretta per un elemento (cioè, legandolo a costi e profitti), a quell'elemento viene spesso data bassa priorità. Le aziende stanno ora scoprendo come la protezione dei dati e i meccanismi di sicurezza influiscono sui loro profitti. Se un'azienda subisce una violazione dei dati, deve affrontare un'ampia gamma di problemi per i quali probabilmente non è preparata. Nel recente passato, un certo numero di aziende ha subìto attacchi ai propri *database* e compromissione delle informazioni sui clienti. Una volta che i clienti scoprono che un'azienda non protegge adeguatamente le loro informazioni riservate e finanziarie, spesso portano la loro attività altrove. Inoltre, i clienti possono citare in giudizio l'azienda, il che potrebbe comportare danni punitivi e onerose spese giudiziarie. Le aziende socialmente responsabili seguono la cosiddetta *due diligence*[218], ovverosia l'atto di indagare e comprendere il

---

[217] PETTERS J. (2020), *Data Privacy Guide: Definitions, Explanations and Legislation*, Varonis. Varonis è un pioniere nella sicurezza dei dati e nell'analisi, che combatte una battaglia diversa rispetto alle società di sicurezza informatica convenzionali. Disponibile *online* al seguente indirizzo *web*: https://www.varonis.com/blog/data-privacy/. Data di ultima consultazione: 9 ottobre 2020.

[218] L'espressione *due diligence* viene in realtà dal latino "*debita diligentia*", cioè investigazione condotta con la diligenza dovuta al caso specifico. L'espressione inglese *due diligence* (in italiano: diligenza dovuta) indica l'attività di investigazione e di approfondimento di dati e di informazioni relative all'oggetto di una trattativa. Il fine di questa attività è quello di valutare la convenienza di un affare e di identificarne i rischi e i problemi connessi, sia per negoziare termini e condizioni del

rischio che l'azienda deve affrontare. Un'azienda pratica la dovuta cura sviluppando e implementando politiche, procedure e *standard* di sicurezza. La dovuta attenzione dimostra che un'azienda si è assunta la responsabilità delle attività che si svolgono all'interno della società e ha preso le misure necessarie per proteggere l'azienda, le sue risorse e i dipendenti da possibili minacce. La *due diligence* è comprendere le minacce e i rischi attuali e la dovuta cura sta implementando contromisure per fornire protezione da tali minacce[219]. Quando una società non pratica la dovuta

---

contratto, sia per predisporre adeguati strumenti di garanzia, di indennizzo o di risarcimento. Cfr. Sentenza del Tribunale di Torino, I sez. civ., 3 marzo 2015. Presidente ed estensore: dott. Marco Ciccarelli.

[219] Come si verifica la solidità di un sistema *privacy* in fase di *due diligence*? Una solida *compliance* deve essere verificata da un punto di vista sostanziale, non formale. Per affrontare una *due diligence* è necessario adottare l'approccio della *privacy by design*. Prima ancora di domandarsi "che cosa richiedere" all'organizzazione che si intende acquistare (con le solite "liste della spesa"), dunque, è necessario domandarsi: "esattamente che cosa sto acquistando?" e ancora "qual è il flusso dei dati che entra e esce dall'organizzazione?". Sarà sulla base della natura dell'azienda che intendo acquistare e sul reale flusso di dati che caratterizza le sue specifiche attività che potrò finalmente stilare la comoda *Check-list* della *due diligence*. La stessa, tra le altre cose, certamente dovrà comprendere: le finalità del trattamento dei dati personali e le conseguenti basi giuridiche; le *policy* aziendali e le procedure che sono state predisposte e adottate (in particolare le procedure di *data breach* e dei diritti degli interessati), le quali danno prova di un reale organizzazione di un *sistema privacy*; il registro delle violazioni (fondamentale al fine di comprendere quali sono state le violazioni dei dati subite dall'organizzazione e come la stessa le abbia gestite); la mappatura dei soggetti esterni (responsabili, contitolari, destinatari) e la relativa documentazione; le misure di sicurezza che sono state implementate sulla base dei rischi effettivi dell'azienda; le valutazioni di impatto necessarie per i trattamenti specifici che svolge l'azienda; l'organigramma interno, con relativa distribuzione delle responsabilità tra il personale e le attività di formazione che sono state messe in atto al fine della necessaria sensibilizzazione; il registro dei

cura o *due diligence* relativa alla sicurezza del proprio patrimonio di dati, può essere legalmente accusata di negligenza e ritenuta responsabile per qualsiasi ramificazione di tale negligenza[220]. La protezione dei dati avviene tramite le pratiche di *privacy*, riservatezza e sicurezza delle informazioni. Come indicato, i dati critici diventano una risorsa per l'azienda. I profitti e le perdite sono determinati dall'integrità dei dati. Avviamento o punizione possono derivare in base a come vengono trattati i dati aziendali. L'intera reputazione di un'azienda potrebbe aumentare o diminuire in base al modo in cui vengono percepiti e gestiti i dati dei clienti[221]. Per tutti questi motivi, il concetto di protezione dei dati è una questione significativa[222]. È stato altresì osservato che le pratiche di *marketing* che si avvalgono dell'analisi dei dati dei consumatori sono avanzate più rapidamente rispetto alla teoria accademica[223]. L'accesso alle informazioni dei

trattamenti. Così DI NUNZIO A. (2020), *Due diligence e privacy: un binomio ormai imprescindibile. Perché e come verificare la compliance dell'azienda*, Studio Legale Stefanelli. Data di ultima consultazione: 13 ottobre 2020. Disponibile *online* al seguente indirizzo *world wide web*: https://www.studiolegalestefanelli.it/it/sharingknowledge/articoli/a/due-diligence-privacy-perche-e-come-verificare-compliance-azienda.

[220] HARRIS S. (2010), *All-In-One CISSP Guide*, 5th Edition, McGraw Hill, USA.

[221] ASHWORTH L., FREE C. (2006), *Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns*, Journal of Business Ethics, 67, 107-123.

[222] MCPHERSON H. (2014), *Data Privacy—Protecting This Asset Is a Priority*, Isaca Journal Archives. Data di ultima consultazione: 10 ottobre 2020. Disponibile *online* al seguente indirizzo *world wide web*: https://www.isaca.org/resources/isaca-journal/pastissues/2014/data-privacy-protecting-this-asset-is-a-priority.

[223] MARTIN K. D., MURPHY P. E. (2017), *The role of data privacy in marketing*, Journal of the Academy of Marketing Science, 45, 135-155. Gli autori forniscono una completa e interessante *literature review* in tema di *data privacy in marketing*. Nel loro *paper* vengono esaminate

consumatori è al centro del paradigma di *marketing* incentrato sul cliente, in quanto consente, ad esempio, l'implementazione di azioni mirate a creare offerte personalizzate di beni o servizi[224]. Sia la letteratura manageriale che quella accademica hanno dimostrato che le aziende che utilizzano strategie basate sui dati sono più redditizie e produttive rispetto ai loro concorrenti[225]. Nel corso degli anni, le persone hanno sempre più condiviso le loro informazioni personali con rivenditori, piattaforme di *social media* e aziende con cui hanno interagito, in cambio dei loro servizi. Le aziende, a loro volta, hanno utilizzato progressivamente questi dati ai fini della profilazione dei propri clienti, per essere in grado di prendere decisioni migliori e creare in maniera più efficiente ed efficace valore attraverso canali sia digitali che non digitali[226]. Studi dimostrano come le persone consapevoli di poter controllare la propria *privacy online* sono più disponibili a fornire informazioni personali e a reagire positivamente

prospettive teoriche e risultati empirici inerenti ai *data privacy*, raggruppati in base al ruolo della *privacy* nella società, nella psicologia e nell'economia. Sintetizzando la letteratura accademica sul tema in queste tre aree, gli autori sostengono un modo di pensare olistico sull'uso organizzativo dei dati dei consumatori e su come si adattano in un quadro sociale più ampio. Con particolare riferimento all'area della economia della *privacy*, o meglio come la imprese gestiscono la *privacy* dei consumatori, la *review* evidenzia che solo un *corpus* limitato di ricerche compone quest'area.

[224] MARTIN K. D., BORAH A., PALMATIER R. W. (2017), *Data privacy: Effects on customer and firm performance*, Journal of Marketing, 81(1), 36-58.

[225] LOHR S. (2012). *Sure, Big Data is Great. But so is intuition*, The New York Times. Disponibile *online* al seguente indirizzo *world wide web*: https://www.nytimes.com/2012/12/30/technology/big-data-is-great-but-dont-forget-intuition.html. Data di ultima consultazione: 16 ottobre 2020.

[226] EDELMAN D. C., SINGER M. (2015), *Competing on customer journeys*, Harvard Business Review, 93(11), 88-100.

agli annunci personalizzati[227]. La fornitura di una chiara informativa comporta un aumento della fiducia e una riduzione delle preoccupazioni relative alla *privacy*, il che influenza positivamente la probabilità di consentire l'accesso ai dati personali[228]. Inoltre, prendendo in considerazione la prospettiva costi-benefici, i ricercatori hanno esaminato se e in che modo le aziende possono superare i costi percepiti associati alla divulgazione dei dati aumentandone i vantaggi percepiti[229]. È stato appurato inoltre che la possibilità di ricevere il consenso alla *privacy* può essere influenzato dall'inquadramento della sua richiesta. Più specificamente, i consumatori sembrano avere maggiori probabilità di concedere il consenso quando la negazione dell'utilizzo dei dati è presentata come una minaccia alla perdita della qualità del servizio rispetto a quando il consenso all'utilizzo dei dati è presentato come un'opportunità per ottenere un servizio migliore[230]. Tuttavia, è stato dimostrato come i consumatori possono facilmente sentirsi maltrattati e provare reattività nel momento in cui le imprese inquadrano la loro richiesta

---

[227] TUCKER C. E. (2014), *Social networks, personalized advertising, and privacy controls*, Journal of Marketing Research, 51(5), 546-562.

[228] ATHEY S., CATALINI C., TUCKER C. (2017), *The digital privacy paradox: small money, small costs, small talk*, National Bureau of Economic Research, Cambridge, MA, Working Paper 23488.

[229] Cfr. KRAFFT M., ARDEN C. M., VERHOEF P. C. (2017), *Permission Marketing and Privacy Concerns—Why Do Customers (Not) Grant Permissions?*, Journal of Interactive Marketing, 39, 39-54; WHITE T. B., ZAHAY D. L., THORBJØRNSEN H., SHAVITT S. (2008), *Getting too personal: Reactance to highly personalized email solicitations*, Marketing Letters, 19(1), 39-50.

[230] WHITE T. B., NOVAK T. P., HOFFMAN D. L. (2014), *No strings attached: When giving it away versus making them pay reduces consumer information disclosure*, Journal of Interactive Marketing, 28(3), 184-195.

come una minaccia per ridurre la qualità del servizio[231]. La sensibilità dei consumatori nei confronti delle informazioni personali sta cambiando a causa dei progressi tecnologici, per cui le informazioni una volta considerate innocue sono ora considerate più sensibili e quindi necessitano di maggiore protezione. Viene riesaminato dunque il concetto di sé e il contesto di scambio come una nuova lente per comprendere la sensibilità del consumatore allo scambio di informazioni di identificazione anonima e personale[232]. Basandosi sugli studi inerenti alla dimensione collettiva della protezione dei dati, è stato addirittura elaborato un modello di valutazione incentrato sui diritti umani: la *Human Rights, Ethical and Social Impact Assessment* (HRESIA). Questo modello di autovalutazione intende superare i limiti dei modelli di valutazione esistenti, i quali sono troppo focalizzati sull'elaborazione dei dati o nell'avere un'estensione e una granularità che li rendono troppo complicati per valutare le conseguenze di un determinato uso dei dati[233].

[231] KU H. H., YANG P. H., CHANG C. L. (2018), *Reminding customers to be loyal: does message framing matter?*, European Journal of Marketing, 52(3/4), 783-810.

[232] MARCOS E., LABRECQUE L. I., MILNE G.R. (2018), *A New Information Lens: The Self-concept and Exchange Context as a Means to Understand Information Sensitivity of Anonymous and Personal Identifying Information*, Journal of Interactive Marketing, 42, 46–62.

[233] MANTELERO A. (2018), *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, Computer Law & Security Review, 34, 754–772.

# CAPITOLO 3

# IL RAPPORTO ETICO TRA PRIVACY E RESPONSABILITÀ SOCIALE D'IMPRESA

**SOMMARIO:** 1. Introduzione – 2. La struttura piramidale della RSI e la risposta aziendale alla privacy – 3. Funzione sociale della protezione dati – 4. Il principio di accountability e gli approcci socialmente responsabili al trattamento dei dati previsti dal GDPR

## 1. Introduzione

La tutela della *privacy* è un diritto fondamentale della persona e una necessità imprescindibile della società moderna. Tuttavia, viene spesso vissuta e interpretata in ambito imprenditoriale come un obbligo burocratico che rallenta o rende più macchinoso il raggiungimento degli obiettivi d'impresa. Ciò anche perché non sempre gli operatori sono a conoscenza delle opportunità e delle modalità semplificate che il Garante per la protezione dei dati personali ha nel tempo indicato per ottenere una conformità sostanziale alla protezione dei dati, evitando il ricorso ad adempimenti inutili e meramente formali. Da un'attenta analisi delle prassi aziendali emerge che la corretta adozione di semplici misure di protezione dei dati personali può contribuire a rendere più efficiente l'organizzazione dell'impresa e a ridurre sensibilmente i potenziali rischi a cui la stessa si espone sul mercato. Nello spirito imprenditoriale, l'adozione di una buona prassi può migliorare non solo l'immagine dell'impresa, come soggetto attento al principio di responsabilità sociale, ma

anche la capacità di *business* a parità di costi sostenuti, aumentando la fiducia di utenti e consumatori nella serietà e affidabilità dell'impresa.

## 2. La struttura piramidale della responsabilità sociale d'impresa e la risposta aziendale alla privacy

Gestire correttamente i dati personali è una responsabilità sociale? La responsabilità sociale si basa sulla legge, sull'azione volontaria o sull'opportunità di mercato? Verso chi l'impresa deve essere responsabile? Sebbene la *privacy* costituisca un filone di studi ampiamente studiato nelle discipline affini alla sociologia, solo recentemente gli studiosi di *marketing* hanno iniziato a interessarsi al tema. La letteratura manageriale sostiene che le imprese possono trarre vantaggio competitivo dalla protezione dei dati, specialmente se questo impegno viene inserito nelle proprie agende di RSI e reso noto agli *stakeholder*[234].

[234] Cfr. sul tema SHARFMAN M. P., PINKSTON T. S. E SIGERSTAD T. D. (2000), *The effects of managerial values on social issues evaluation: an empirical examination*, Business and Society, 39(2), 144–182, i quali propongono un sondaggio tra i dirigenti su quanto sia importante considerare una serie di problemi sociali, tra cui la protezione della *privacy*; FUKUKAWA K. E MOON J. (2004), *A Japanese model of corporate social responsibility? A study of website reporting*, Journal of Corporate Citizenship, 16, 45–59, i quali includono la *privacy* come indicatore di RSI nel loro studio condotto su imprese in Giappone; CHAUDHRI V. A. (2006), *Organising global CSR: a case study of Hewlett-Packard's e-inclusion initiative*, Journal of Corporate Citizenship, 23, 39–51, menziona la *privacy* come un'area che l'impresa oggetto di studio ha incluso nella sua agenda di RSI; CARROLL A. B. (1998), *The four faces of corporate citizenship*, Business and Society Review, 100(1), 1–7, che evidenzia la protezione dei diritti della *privacy online* come area in cui la legge è in ritardo rispetto al pensiero etico ed entra in gioco la

Solamente pochi studi di *business ethics* hanno affrontato il collegamento tra *information privacy* e *corporate social responsibility*[235]. La protezione dei dati non è da considerare una mera conformità giuridica: difatti, viene sempre più concepita come una importante responsabilità sociale che apporta vantaggio competitivo alle imprese nella gestione strategica e benefici ai consumatori, che mostrano preferenza per la riservatezza dei loro dati. Carroll è stato il primo autore a introdurre il tema della responsabilità sociale d'impresa nelle teorie di *management* (1979). L'autore, concentrandosi sulla classificazione delle relazioni che possono intercorrere tra impresa e società, ha teorizzato il modello della Piramide della Responsabilità Sociale d'Impresa (1991), secondo cui l'impresa ha quattro livelli di responsabilità posti in ordine gerarchico crescente: 1. economica, 2. legale, 3. etica, e 4. filantropica[236].

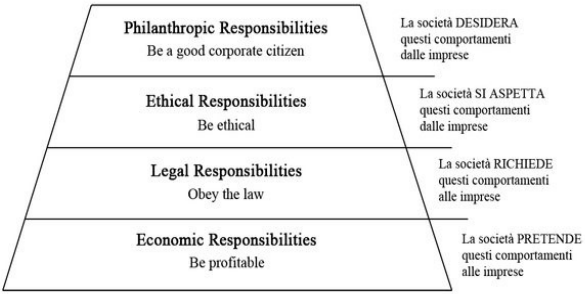
---

moralità; POST J. E. (2000), *Moving from geographic to virtual communities: global corporate citizenship in a dot.com world*, Business and Society Review, 105(1), 27–46, che ha esaminato il cambiamento del ruolo della *corporate citizenship* nel XXI secolo e ha indicato la *privacy* dei clienti come una nuova questione di RSI.

[235] POLLACH I. (2011), *Online privacy as a corporate social responsibility: an empirical study*, Business Ethics: A European Review, 20(1), 88-102. Sulla base di uno studio di divulgazione di CSR, l'articolo contribuisce alla letteratura esistente esplorando se e come le più grandi aziende di *Information Technology* (IT) abbracciano la *privacy online* come CSR. I risultati dello studio indicano che solo una piccola parte delle aziende del campione ha programmi globali sulla *privacy*, sebbene più della metà di esse esprimano motivi morali o relazionali per affrontare la *privacy online*. Le misure *privacy* che hanno adottato sono principalmente misure di conformità, mentre le misure che stimolano il dialogo con gli *stakeholder* sono rare. Lo studio conclude sostenendo che la *privacy online* era piuttosto nuova nell'agenda della CSR e che giocava solo a ruolo secondario (2011).

[236] CARROLL A. B. (1979), *A three-dimensional conceptual model of corporate performance*, Academy of Management Review, 4(4), 497-

**Figura 1. La Piramide della Responsabilità Sociale d'Impresa (Carroll, 1991)**




Il modello pone al primo stadio le responsabilità di creare valore economico per gli azionisti e valore in termini di offerta di beni e servizi per il mercato (*be profitable*). In altri termini, la responsabilità posta alla base permette agli *stakeholder* primari o ai soggetti di istituto di avere remunerazioni in equilibrio rispetto ai contributi; così facendo non si corre il rischio che gli stessi percepiscano nessun rendimento e abbandonino l'azienda. Al contempo si richiede alle imprese di produrre beni e servizi vendendoli alla società ad un prezzo equo. La responsabilità legale (*obey the law*), posta al secondo livello e dunque al gradino successivo, consiste nel rispetto totale e assoluto della legislazione che la società richiede nei Paesi in cui opera l'impresa. Più vicino al vertice vi è la responsabilità etica (*be ethical*), ossia la conformità al sistema di princìpi, valori e norme sociali (equità, giustizia, imparzialità) e infine, al vertice, la responsabilità filantropica (*be a good corporate citizen*), vale a dire l'impegno da parte dell'impresa in investimenti a favore

505; CARROLL A. B. (1991), *The pyramid of corporate social responsibility: Toward the moral management of organizational stakeholders*, Business Horizons, 34(4), 39-48.

della comunità. Queste ultime due responsabilità sono discrezionali e liberamente scelte dalle imprese. Carroll sostiene che la realizzazione del profitto è la responsabilità per eccellenza delle imprese, insieme alla loro aderenza alle normative legali: i primi due livelli sono considerati dunque necessari, mentre il terzo atteso dalla comunità e il quarto risulta essere discrezionale. Grazie a questo modello, i concetti di volontarietà e discrezionalità vengono introdotti per la prima volta nelle attività filantropiche, risultando essere una novità assoluta nel campo di studi. Data la classificazione riportata in *Figura 1*, la protezione dei dati può essere classificata come responsabilità etica qualora la legislazione non sia sufficiente a controllare il processo decisionale delle imprese in tutte le aree del trattamento dei dati[237]. Se l'impresa decidesse di abbracciare la protezione dei dati potrebbe farlo per altre questioni, non solo per responsabilità etica. Difatti, le imprese accolgono questo importante impegno per questioni sociali riconducibili alle responsabilità filantropiche, ciò sostanzialmente per tre diversi motivi: (1) ragioni morali determinati dai valori legati alla moralità; (2) ragioni relazionali, determinate dalla preoccupazione dell'impresa in merito alle relazioni con gli *stakeholder*; e (3) ragioni strumentali, guidate dall'interesse personale dell'impresa[238]. Quanto a

[237] Cfr. MINTZBERG H. (1983), *The case for corporate social responsibility*, Journal of Business Strategy, 4(2), 3-15. L'autore ha indicato che le aree in cui la CSR entra in gioco sono quelle '*where existing legislation needs compliance with its spirit as well as its letter [and] where the corporation can fool its customers or suppliers or the government through its superior knowledge*' (p. 12).

[238] AGUILERA R.V., RUPP D., WILLIAMS C.A., GANAPATHI J. (2007), *Putting the S back in CSR: a multilevel theory of social change in organizations*, Academy of Management Review, 32(3), 836–863. Secondo gli autori, (1) i motivi morali sono messi in atto in particolare da individui con potere decisionale organizzativo che hanno forti valori basati sulla

quest'ultimo approccio, le imprese che riescono a guadagnare la fiducia dei propri *stakeholder* sono in grado di garantire un vantaggio competitivo attraverso risparmi sul monitoraggio dei costi, costi di legame, costi di transazione e i costi di ricerca derivanti dalla gestione dei vari gruppi di *stakeholder* aziendali[239]. La letteratura accademica segue generalmente l'approccio strumentale alla responsabilità sociale d'impresa, sostenendo che le imprese in cui una particolare responsabilità è molto rilevante possono trarre vantaggio dall'integrazione di questa responsabilità nelle loro strategie generali. Le condizioni affinché la RSI possa apportare vantaggi strategici per l'impresa sono molteplici; in questo contesto, il tema della RSI deve: essere centrale nella *mission* aziendale, abbracciato volontariamente, portare benefici sia all'impresa che al pubblico, essere indirizzato in maniera proattiva e visibile agli *stakeholder* esterni[240]. La letteratura documenta anche le crescenti preoccupazioni dei consumatori sulla violazione della *privacy* nelle transazioni *online* che derivano sostanzialmente dallo squilibrio di potere tra le imprese (come raccoglitori di dati) e utenti (come fornitori di dati)[241]. Per far fronte alle

---

moralità; (2) i motivi relazionali sono radicati nel desiderio di un'impresa di promuovere e bilanciare gli interessi degli *stakeholder*, creando così fiducia, massimizzando la ricchezza degli stakeholder e guadagnando legittimità sociale; (3) gli approcci strumentali sono determinati dall'interesse personale, cercando di raggiungere una maggiore competitività e protezione della reputazione aziendale.

[239] JONES T. M. (1995), *Instrumental stakeholder theory: a synthesis of ethics and economics*, Academy of Management Review, 20(2), 404–437.

[240] BURKE L., LOGSDON J. M. (1996), *How corporate social responsibility pays off*, Long Range Planning, 29(4), 495–502.

[241] Cfr. sul tema CULNAN M. J., ARMSTRONG P. K. (1999), *Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation*, Organization Science, 10(1), 104–115; PHELPS J.,

nuove esigenze del consumatore, a partire dal nuovo millennio alcune imprese hanno iniziato a introdurre la figura del *Chief Privacy Officer*[242] i cui compiti includono la raccolta di informazioni sugli aspetti sociali e legali della *privacy*, l'ideazione della strategia sulla *privacy* aziendale, la diffusione di informazioni sulle pratiche di gestione dei dati aziendali agli *stakeholder* interni ed esterni, e la rappresentanza dell'impegno dell'impresa per la *privacy*[243]. Una gestione integrata della RSI implica l'inserimento di prassi socialmente responsabili nella pianificazione strategica e delle operazioni aziendali quotidiane. In altri termini, la responsabilità sociale prescrive alle imprese di assumere un comportamento responsabile nei confronti di ciascuno dei propri *stakeholder*. Tale integrazione influenza tutti gli ambiti della gestione, dalla produzione al *marketing*, dalla gestione delle risorse umane agli aspetti finanziari e di controllo dei rischi. Definire opportune politiche di RSI implica, in primo luogo, l'identificazione dei punti di interdipendenza tra impresa e società, e, in secondo luogo, la scelta delle questioni sociali di cui occuparsi e la definizione dell'agenda sociale dell'impresa, coniugando le politiche di RSI legate alla catena del valore con quelle derivanti dal contesto competitivo. Infine, la

---

NOWAK G., FERRELL E. (2000), *Privacy concerns and consumer willingness to provide personal information*, Journal of Public Policy and Marketing, 19(1), 27–41; SHEEHAN K. B. (2002), *Toward a typology of internet users and online privacy concerns*, The Information Society, 18(1), 21–32; NORBERG P. A., HORNE D. R. (2007), *Privacy attitudes and privacy-related behavior*, Psychology and Marketing, 24(10), 829–847; NORBERG P. A., HORNE D. R., HORNE D. A. (2007), *The privacy paradox: personal information disclosure intentions versus behaviors*, Journal of Consumer Affairs, 41(1), 100–126.

[242] AWAZU Y., DESOUZA K. C. (2004), *The knowledge chiefs: CKOs, CLOs and CPOs*, European Management Journal, 22(3), 339–344.

[243] KAYWORTH T., BROCATO L., WHITTEN D. (2005), *What is a chief privacy officer?*, Communications of AIS, 16, 110–126.

dimensione sociale viene inclusa nella *value proposition*, in modo che l'impatto sociale sia parte integrante della strategia d'impresa[244]. Integrare la RSI nella gestione quotidiana della catena del valore significa mettere in atto un circolo virtuoso tra comportamento socialmente responsabile ed efficienza aziendale. Si tratta di un modo di guardare al benessere sociale e al profitto economico non più come un gioco a somma zero ma come un mutuo guadagno[245]. In quest'ottica, la RSI viene vista come un investimento[246] finalizzato alla produzione di vantaggi competitivi duraturi e alla minimizzazione dei rischi. Le pratiche di gestione responsabile al trattamento dei dati personali si rivelerebbero, pertanto, uno strumento in grado di apportare effetti positivi sulla *performance* globale di impresa. Una consapevole gestione della reputazione e dell'immagine aziendale sono strumenti fondamentali per garantire legittimazione sociale e consenso, necessari ad assicurare il mantenimento delle relazioni nel tempo e lo sviluppo di un vantaggio competitivo. Nonostante le pratiche di responsabilità sociale offrano alle imprese importanti benefici, ad esempio ottenere un vantaggio competitivo aumentando la consapevolezza del *brand* e quindi aumentando la redditività a lungo termine, queste richiedono risorse finanziarie aggiuntive. La letteratura accademica conferma inoltre le opportunità[247] apportate

---

[244] PERRINI F., TENCATI A. (2008), *Corporate social responsibility. Un nuovo approccio strategico alla gestione d'impresa*, Milano, Egea.

[245] PORTER M. E., KRAMER M. R. (2006), *Strategy & society: the link between competitive advantage and corporate social responsibility*, Harvard Business Review, 84, 78–92.

[246] Sul punto cfr. il contributo di ANDERSON J. (1987), *Can social responsibility be handled as a corporate investment?,* Business Horizons, 24-25.

[247] Cfr. studi che hanno approfondito il ruolo della RSI su crisi di diversa natura: FERNÁNDEZ B., SOUTO F. (2009), *Crisis and Corporate Social Responsibility: Threat or Opportunity?*, International Journal of

dalle iniziative di RSI in seguito a periodi di crisi di diversa natura: oggigiorno si tratta di una necessità per tutte le imprese, sebbene non allo stesso livello, poiché la crisi economica ha effetti diversi sui quattro livelli di RSI. L'impatto della crisi sulla piramide della RSI di Carroll è riassunto in due proposizioni[248]: 1. la prima sostiene che la crisi costituisce una minaccia per le dimensioni di responsabilità situate alla base della piramide (economica e legale); 2. la seconda sostiene che la crisi rappresenta un'opportunità per le dimensioni di responsabilità situate nella parte superiore della piramide (etica e filantropica). Alla luce di questi razionali, la protezione dei dati si configura sempre più come pretesa di carattere universale e indiscutibilmente una nuova ed efficace forma di responsabilità sociale per le imprese che, affidandosi a ragioni etiche e filantropiche, riescono a coglierne il potenziale: al centro dell'attenzione, oltre al dato in sé, vi è la figura del titolare del trattamento.

---

Economic Sciences and Applied Research, 2(1), 36-50; GIANNARAKIS G., THEOTOKAS I. (2011), *The Effect of Financial Crisis in Corporate Social Responsibility Performance*, International Journal of Marketing Studies, 3(1), 1-10; JACOB C. K. (2012), *The Impact of Financial Crisis on Corporate Social Responsibility and Its Implications for Reputation Risk Management*, Journal of Sustainability Science and Management 2(2), 259-275; TEE E., ASARE L. B., OPOKU R. T., TABITHA O. (2017), *The Effect of the 2008 Financial Crisis on Corporate Social Responsibilities: Evidence from Multinational Companies*, Research Journal of Finance and Accounting, 8(16), 20-30; CHUNG L., WEI C. (2017), *The Impact Effect of Corporate Governance and Corporate Social Responsibility on Company Performance After the Financial Tsunami*, Asian Journal of Economic Modelling, 5(4), 465-479.

[248] YELKIKALAN N., KÖSE C. (2012), *The effects of the financial crisis on corporate social responsibility*, International Journal of Business and Social Science, 3(3), 292-300.

## 3. Funzione sociale della protezione dati

La nuova normativa in materia di protezione dati impone un sistema basato sulla responsabilità e impostato su una serie di obblighi in capo al titolare del trattamento, consistenti in obblighi generali (art. 24) e obblighi concernenti la sicurezza di tipo preventivo e successivo (artt. 32 ss.), nonché adempimenti di valutazione d'impatto e consultazione preventiva (artt. 35 ss.), cui si aggiungono le disposizioni di *privacy by design* e *privacy by default*, intesi come strumenti di protezione *ex ante* e *life-long* dei dati. Il legislatore europeo non ha inteso meramente caricare di nuovi compiti titolari e responsabili del trattamento dei dati[249], quanto piuttosto coinvolgerli in un processo volto a erogare beni e servizi *privacy oriented*, sulla base di un mutamento di prospettiva che intenda la protezione dati come valore piuttosto che come costo, delineando un sistema di regole nel segno di un contemperamento tra i diritti dell'interessato e quello del titolare ad espletare il trattamento senza scontare il peso di adempimenti e costi sproporzionati rispetto al tipo di attività svolta[250]. Il nuovo approccio al rischio (*risk-oriented approach*) appare tutto incentrato nella sfera del titolare, nelle declinazioni di una maggiore proceduralizzazione degli obblighi dello stesso e del

[249] Cfr. Parere 3/2010, punto 35. Il Gruppo di lavoro Articolo 29 rileva che alcuni responsabili del trattamento potrebbero percepire il principio generale di responsabilità come un'onerosa imposizione di nuovi obblighi giuridici in capo ai responsabili del trattamento, in particolare vista l'attuale difficile situazione economica dell'UE. Quest'interpretazione non sarebbe corretta.

[250] Si veda BRAVO F. (2018), *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, CEDAM, Padova, per una lettura del sistema che attribuisce rilievo al potere/diritto del titolare a svolgere il trattamento.

principio di *accountability*, che si traduce in *compliance* dei trattamenti. Tale architettura giuridica dei meccanismi di responsabilità prevede due livelli, dei quali il primo è costituito da un obbligo di base vincolante per tutti i titolari del trattamento, consistente nell'attuazione di misure e procedure e nella conservazione delle relative prove, mentre il secondo livello include sistemi di responsabilità di natura volontaria eccedenti le norme di legge minima, in relazione ai princìpi fondamentali di protezione dei dati (tali da fornire garanzie più elevate di quelle prescritte dalla normativa vigente) e/o intermedi modalità di attuazione di garanzia dell'efficacia delle misure (norme di attuazione) e consistente nell'obbligo di conformarsi[251]. Un'impresa che adotti un comportamento socialmente responsabile, valutando e rispondendo alle aspettative economiche, ambientali e sociali di tutti gli *stakeholders* travalicando il minimo impregno previsto dalla legge, coglie l'obiettivo di creare valore e conseguire un vantaggio competitivo. Al contrario, comportamenti poco etici o la mancanza di strategie di sostenibilità e responsabilità sociale delle imprese possono danneggiare la reputazione di un'azienda e renderla meno attraente per gli azionisti, con conseguente riduzione dei profitti. In altri termini, qualora le imprese decidessero spontaneamente di aderire alla RSI, non si limiteranno a soddisfare gli obblighi giuridici, ma potranno andare oltre investendo ulteriormente nel capitale umano e nei rapporti con gli *stakeholders*. La inevitabile conseguenza è il mutamento del ruolo e della concezione dell'impresa stessa: si assiste al passaggio dalla logica del profitto e dello sviluppo a discapito della società civile alla visione eticamente orientata dell'attività di impresa. Le imprese, in quanto organi dello Stato-comunità, avrebbero

[251] MOLLO F. (2019), *Gli obblighi previsti in funzione di protezione dei dati personali*, in ZORZI GALGANO N. (a cura di) (2019), op. cit., p. 257 ss.

il compito di promuovere lo sviluppo ed il benessere della comunità stessa attraverso la soddisfazione degli interessi del consumatore e del lavoratore, pena l'assunzione di responsabilità etica nei confronti della stessa collettività[252]. Il Regolamento UE 2016/679 si fonda sull'idea che le attività di trattamento dei dati debbano essere rivolte al servizio dell'uomo in un'ottica di tutela globale e complessiva. Da questo assunto discende che il diritto alla protezione dei dati non è un diritto assoluto, ma un diritto che viene riconosciuto per la sua funzione sociale[253] e che va, pertanto, contemperato di volta in volta con gli altri diritti fondamentali dell'uomo rilevanti e prevalenti, come, ad esempio, il diritto alla libertà di espressione o il diritto al rispetto della vita privata e familiare. La scelta del legislatore europeo di affermare, in un *considerando* iniziale di un atto direttamente applicabile in tutti gli Stati membri dell'Unione Europea, che il diritto alla protezione dei dati personali non è una prerogativa assoluta e che è necessario considerare la sua «funzione sociale» attesta la volontà di sancire un principio di valenza generale su cui si fonda l'impianto normativo e un criterio argomentativo cui

[252] PFOESTL E. (a cura di) (2012), *La responsabilità sociale di impresa, sviluppo, sostenibilità ed economia sociale di mercato,* Editrice Apes, Roma, p. 61.

[253] Cfr. Considerando 4 GDPR: (4) Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. 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. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.

va orientata l'interpretazione e la concreta applicazione delle regole[254]. Il diritto alla protezione dei dati personali è assoluto, nella misura in cui è riconosciuto a chiunque, garantito solo nell'interesse della persona cui si riferisce e vantabile nei confronti di tutti; è relativo, nella misura in cui possono presentarsi vincoli esterni, tali da restringere o limitare l'esercizio delle pretese. All'affermazione secondo cui il diritto alla protezione dei dati personali non è una prerogativa assoluta si affianca quella per cui questo diritto va considerato alla luce della sua «funzione sociale». La funzione va riferita alle informazioni oggetto della pretesa individuale. Sotto il profilo ontologico, la funzione riferita al diritto alla protezione dei dati personali è un limite al complesso delle pretese vantabili dall'interessato, giustificabile in ragione dell'oggetto del diritto che nel caso è il dato personale. Se il dato personale è funzionale al soddisfacimento di un interesse che supera i confini della sfera individuale dell'interessato, la limitazione della prerogativa sul medesimo dato è legittima[255]. La formula della funzione sociale, ovvero della funzione nella società, si pone quindi come criterio argomentativo in cui declinare l'affermata relatività del diritto alla protezione dei dati

[254] RICCI A. (2017), *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, Contratto e impresa. Dialoghi con la giurisprudenza civile e commerciale, 2, Cedam, pp. 587-612.

[255] Sulla necessità di modellare la disciplina normativa alla luce della funzione del dato v. RODOTÀ S. (1985), *Circolazione delle informazioni e protezione dei dati personali*, in AA.VV., *Il diritto delle comunicazioni di massa. Problemi e tendenze*, a cura di ROPPO V., Cedam, Padova, p. 225, che già prima dell'entrata in vigore della dir. 95/46/CE ha prospettato la necessità che «la difesa della *privacy* superi la logica puramente proprietaria, integrando i controlli individuali con quelli collettivi, differenziando la disciplina a seconda delle funzioni a cui le informazioni raccolte sono destinate, analizzando (…) gli interessi coinvolti nelle diverse operazioni e mettendo a punto nuovi criteri per il bilanciamento di tali interessi».

personali. L'assolutezza del diritto alla protezione dei dati personali trova nella funzione sociale un principio alla stregua del quale coordinare fra loro la pretesa dell'interessato, gli interessi dei titolari del trattamento, le esigenze avvertite dalla società nel suo insieme[256]. Essa non può che riferirsi all'oggetto del diritto e non può che essere interpretata come criterio di temperamento fra pretese individuali ed interessi generali. Il contemperamento degli interessi, cui è preordinata la formula della funzione sociale, è connaturale alla duplice valenza del dato personale: da un lato, elemento essenziale per la libera circolazione delle persone, dei beni e dei servizi; dall'altro, componente dell'identità personale, strumento di esplicazione della personalità e di esercizio delle libertà individuali. Il contemperamento degli interessi è quindi la conseguenza del connotato sociale del dato, che non si identifica necessariamente in uno scopo di pubblica utilità.

## 4. Il principio di accountability e gli approcci socialmente responsabili al trattamento dei dati previsti dal General Data Protection Regulation

Il Regolamento Europeo n. 679 del 2016 (*General Data Protection Regulation* – GDPR) pone l'accento sulla responsabilizzazione dei titolari e dei responsabili del trattamento dei dati personali[257], ossia sull' adozione di

[256] RICCI A. (2017), *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, Contratto e impresa. Dialoghi con la giurisprudenza civile e commerciale, 2, Cedam, pp. 587-612.

[257] Cfr., sul punto, GRECO L. (2017), *I ruoli: titolare e responsabile*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, diretto da FINOCCHIARO G. D., Zanichelli, Bologna, in particolare p. 279.

comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento (artt. 23-25 e Capo IV). Dunque, viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento[258].
Il Regolamento – all'articolo 5, paragrafo 2 – richiede al titolare di rispettare i princìpi generali del trattamento dei dati personali e di essere "in grado di comprovarlo". Questo è il principio detto di "responsabilizzazione"[259] (o *accountability*) che viene poi esplicitato ulteriormente dall'articolo 24, paragrafo 1, del Regolamento, dove si afferma che "il titolare 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". Dato che il Regolamento pone l'accento sulla "responsabilizzazione" di titolari e responsabili, ossia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento (artt. 23-25, in particolare, e l'intero Capo IV del

[258] Cfr. per ulteriori approfondimenti sul tema il sito *web* del Garante per la protezione dei dati personali (https://www.garanteprivacy.it) e più specificatamente la sezione "Doveri - Come trattare correttamente i dati", disponibile *online* al seguente indirizzo *web*: https://www.garanteprivacy.it/home/doveri. Data di ultimo accesso e consultazione: 11 giugno 2020.

[259] Precisa giustamente MOLLO F. (2019), *Gli obblighi previsti in funzione di protezione dei dati personali*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, (a cura di) ZORZI GALGANO N., Cedam, Padova, p. 258, che si tratta di un termine che può essere tradotto in molti modi, fra cui responsabilità, affidabilità, assicurazione, obbligo di rendicontazione, attuazione dei principi concernenti il trattamento dei dati personali. Cfr. le precisazioni contenute in Articolo 29 - WP173 - Parere 3/2010 sul principio di responsabilità (punti 21 e 22).

Regolamento), viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento. Il primo fra tali criteri è sintetizzato dall'espressione inglese "*data protection by default and by design*" (articolo 25), ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del Regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto previsto dall'articolo 25, paragrafo 1, del Regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili. Fondamentali fra tali attività sono quelle connesse al secondo criterio individuato nel Regolamento rispetto alla gestione degli obblighi dei titolari: ossia il rischio inerente al trattamento. Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (*considerando* 75-77); tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (artt. 35- 36) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi[260]. Il Regolamento definisce caratteristiche

[260] Cfr. al riguardo le linee guida in materia di valutazione di impatto sulla protezione dei dati del Gruppo "Articolo 29". Data di ultimo accesso e consultazione: 29 luglio 2020. Disponibili *online* al seguente indirizzo *web*: http://www.garanteprivacy.it/Regolamentoue/DPIA. La

soggettive e responsabilità di titolare e responsabile del trattamento[261] negli stessi termini di cui alla direttiva 95/46/CE e, quindi, al Codice *privacy* italiano. Tuttavia, il Regolamento (articolo 28) prevede dettagliatamente le caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento attribuendogli specifici compiti. Deve trattarsi, infatti, di un contratto (o altro atto giuridico conforme al diritto nazionale) e deve disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'articolo 28 al fine di dimostrare che il responsabile fornisce "garanzie sufficienti", quali, in particolare: la natura, durata e finalità del trattamento o dei trattamenti assegnati, le categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel Regolamento. Inoltre, il Regolamento prevede obblighi specifici in capo ai responsabili del trattamento, distinti da quelli pertinenti ai rispettivi titolari. Ciò riguarda, in particolare: la tenuta del registro dei trattamenti svolti (articolo 30, paragrafo 2); l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti (articolo 32); la designazione di un RPD-DPO, nei casi previsti dal

pagina contiene *link* alla normativa e a documenti interpretativi, schede informative e pagine tematiche.

[261] A differenza della precedente direttiva, che prevedeva il solo caso in cui titolari congiunti determinassero un trattamento in eguale misura, rispondendone in ragione della stessa, la nuova disciplina, oltre a disciplinare espressamente la figura del contitolare all'art. 26, prevede la possibilità che la titolarità congiunta non importi necessariamente una pari responsabilità tra i soggetti, ma che possa assumere diverse e varie forme. Sul punto, cfr. PELINO E. (2016), *I soggetti del trattamento*, in BOLOGNINI L., PELINO E., BISTOLFI C. (2016) (a cura di), *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè Editore, Milano, p. 136, che distingue tra contitolarità simmetrica e asimmetrica.

Regolamento o dal diritto nazionale (articolo 37). Una novità importante del Regolamento è la possibilità di designare sub-responsabili del trattamento da parte di un responsabile (articolo 28, paragrafo 4), per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest'ultimo risponde dinanzi al titolare dello inadempimento dell'eventuale sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" (articolo 82, paragrafo 1 e paragrafo 3)[262].

### *4.1 Il registro delle attività di trattamento*

Tutti i titolari e i responsabili del trattamento dei dati personali, eccettuati gli organismi con meno di 250 dipendenti – ma solo se non effettuano trattamenti a rischio (articolo 30, paragrafo 5) – devono tenere un registro delle operazioni di trattamento[263], i cui contenuti sono indicati all'articolo 30. Si tratta di uno strumento fondamentale allo scopo di disporre di un quadro aggiornato dei trattamenti

[262] Cfr. in merito al principio di responsabilizzazione l'ampia letteratura giuridica: DI CARNABUCI A., CECCOLI P., DE ROSA B., MARIANI I., MINIERI C., RADAELLI P., ZAPPIA A., ZUCCHETTI A. (2018), *Privacy e dati personali: Problemi e casi pratici*, Key Editore, Milano, p. 22 ss.; SALA M. (2018), *Privacy. Guida alla lettura del Regolamento (UE) 2016/679 sulla protezione dei dati e del Codice Privacy italiano*, G. Giappichelli Editore, Torino, p. 52 ss.; DE STEFANI F. (2018), *Le regole della privacy: Guida pratica al nuovo GDPR*, HOEPLI, Milano; FABIANO N. (2019), *GDPR & privacy: consapevolezza e opportunità. Analisi ragionata della protezione dei dati personali tra etica e cybersecurity*, goWare, Firenze.

[263] Per approfondimenti sul Registro delle attività di trattamento cfr. il sito *web* del Garante della protezione dei dati personali (https://www.garanteprivacy.it/regolamentoue/registro).

in essere all'interno di un'azienda o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio. Niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno nell'ottica della complessiva valutazione di impatto dei trattamenti svolti. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante. I registri delle attività di trattamento vanno a comporre l'apparato documentale che dimostra la conformità e dà sostanza alla responsabilizzazione. La tenuta del registro costituisce un adempimento formale, sostitutivo, nell'ordinamento italiano, l'obbligo di notificare il trattamento all'Autorità Garante[264]. L'adempimento è strettamente collegato alla valutazione di impatto *privacy* ed è funzionale alla definizione delle misure di sicurezza dei trattamenti[265].

### *4.2 Il Data Protection Officer*

Il responsabile della protezione dei dati (RPD), o anche in inglese *Data Protection Officer* (DPO)[266], è la nuova figura

[264] Per una lettura dettagliata in merito alla disciplina, alla attività, alle modalità di tenuta, agli obblighi e alle sanzioni che ruotano attorno al Registro delle attività di trattamento, cfr. ARNABOLDI N., FERRARA F. G. (2019), *Come compilare il registro delle attività di trattamento dati*, Maggioli Editore, Santarcangelo di Romagna.

[265] CICCIA MESSINA A., BERNARDI N. (2017), *Privacy e Regolamento Europeo*, IPSOA, Milano, pp. 108-109.

[266] Il DPO era stato già introdotto come obbligatorio in alcuni Stati europei, come la Germania (il *datenschutzbeauftragter*, introdotto con il *Bundesdatenschutzgesetz* del 2003, in presenza di dieci dipendenti che utilizzino strumenti manuali, oltre che nei casi in cui il trattamento abbia ad oggetto particolari categorie di dati), l'Austria e la Repubblica Ceca, e come facoltativo in altri, ad esempio la Francia. In data 14 agosto 2018 il Brasile ha approvato una legge (entrata in vigore nel

prevista dall'art. 37. La normativa è stabilita dagli articoli 37 (designazione), 38 e 39 (caratteristiche soggettive e oggettive di questa figura: indipendenza, autorevolezza, competenze manageriali)[267] ed è sintetizzata dal *considerando* 97 del Regolamento UE nr. 2016/679. Il responsabile del trattamento e il responsabile per la protezione dei dati sono due figure ben distinte; difatti, il responsabile del trattamento (art. 28) continua a essere colui che tratta i dati per conto del titolare del trattamento. Il RPD è un soggetto designato dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento stesso. Coopera con l'Autorità Garante alla quale deve essere comunicato il nominativo; costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali. Nell'esercizio dei propri compiti, il RPD considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. Come chiarito nelle Linee Guida del Gruppo di lavoro Articolo 29[268], i RPD non rispondono personalmente in

2020) ampiamente ispirata al Regolamento EU 2016/679: sono state così introdotte nuove figure come ad es. il *Data Protection Officer*.

[267] Per maggiori delucidazioni unitamente alle relative FAQ si rinvia alle linee guida del Gruppo di lavoro "Articolo 29" disponibili anche sul sito *web* del Garante *privacy.* Data di ultimo accesso e consultazione: 25 luglio 2020 (www.garanteprivacy.it/Regolamentoue/rpd).

[268] Il Gruppo dell'articolo 29 per la tutela dei dati (in inglese Article 29 Working Party o WP29) era il gruppo di lavoro comune della autorità nazionali di vigilanza e protezione dei dati. Era un organismo consultivo indipendente, composto da un rappresentante delle varie autorità nazionali, dal Garante europeo della protezione dei dati e da un rappresentante della Commissione. Il presidente era eletto dal Gruppo al suo interno ed ha un mandato di due anni, rinnovabile una sola volta. Il Gruppo adottava le sue decisioni a maggioranza semplice dei

caso di inosservanza del GDPR. Spetta al titolare del trattamento (o al responsabile del trattamento) garantire ed essere in grado di dimostrare che le operazioni di trattamento sono conformi alle disposizioni del Regolamento medesimo (art. 24, paragrafo 1). L'articolo 35 del Regolamento prevede che il responsabile della protezione dei dati sia consultato per la valutazione d'impatto, dovendo fornire un parere (art. 39). Non sono richieste specifiche attestazioni formali o l'iscrizione ad appositi albi. Ciononostante, il RPD deve possedere un'approfondita conoscenza della normativa e delle prassi in materia di *privacy*, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento. Inoltre, deve poter offrire, con il grado di professionalità adeguato alla complessità del lavoro da svolgere, la consulenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali. Il RPD agisce in piena indipendenza e autonomia riferendo direttamente ai vertici e per l'esercizio

---

rappresentanti delle autorità di controllo. L'articolo 29 della direttiva europea 95/46 prevede, vari compiti da affidare ai membri dei Garanti nazionali, che quindi si riunivano per garantire regole comuni in tema di *privacy*. Le sue principali missioni erano: (a) fornire un parere esperto agli Stati in merito alla protezione dei dati; (b) promuovere l'applicazione coerente della direttiva sulla protezione dei dati in tutti gli Stati membri dell'UE, nonché in Norvegia, Liechtenstein e Islanda; (c) dare alla Commissione un parere sulle leggi comunitarie (primo pilastro) che riguardano il diritto alla protezione dei dati personali; (d) fornire raccomandazioni al pubblico su questioni relative alla protezione delle persone con riguardo al trattamento dei dati personali e alla *privacy* nella Comunità europea. Il 25 maggio 2018 è stato sostituito dal Comitato europeo per la protezione dei dati (EDPB) ai sensi del regolamento generale sulla protezione dei dati dell'UE (GDPR) (regolamento (UE) 2016/679). Per ulteriori approfondimenti si consulti il sito *web* della European Data Protection Board (EDPB), disponibile *online* al seguente indirizzo *web*: https://edpb.europa.eu/edpb_en.

della propria funzione deve poter disporre di risorse adeguate (personale, locali, attrezzature, ecc.)[269]. Ai sensi del paragrafo 1 dell'art. 37, il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta: a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; 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. Il paragrafo 4 dell'art. 37 dichiara che il diritto dell'Unione o degli Stati membri può prevedere ulteriori casi di designazione obbligatoria del RPD. Dunque, la nomina è obbligatoria nei tre casi sopraccitati. Solo nel caso delle Pubbliche Amministrazioni, con eccezione delle autorità giurisdizionali nell'esercizio delle loro funzioni, la nomina è chiaramente delineata. Gli altri due casi, vale a dire quelli che riguardano il settore privato, danno adito a gravi incertezze interpretative e operative. Risulta quindi necessario interpretare i concetti di «*core business*», «larga scala» e «monitoraggio regolare e sistematico». Le Linee Guida del Gruppo di lavoro Articolo 29 stabiliscono che per *core business* del titolare o del responsabile del

[269] Per una disamina dei compiti, delle competenze e caratteristiche del responsabile della protezione dati si veda AVITABILE A. (2017), *Il data protection officer*, in *Il nuovo Regolamento sulla privacy e sulla protezione dei dati personali*, diretto da FINOCCHIARO G. D., Zanichelli, Bologna, p. 331 ss.

trattamento si intende una o più attività necessaria per raggiungere lo scopo del titolare o responsabile: si tratta sostanzialmente della principale attività. Ad esempio, il *core business* di una azienda ospedaliera è quello di provvedere alla cura delle persone fisiche e il trattamento dei loro dati è un aspetto necessario all'erogazione del servizio. Per quanto riguarda il concetto di larga scala, il Regolamento non fornisce una definizione chiara, e nonostante le indicazioni del *considerando* 91 è difficile dare una definizione univoca: le linee guida chiariscono che non è possibile dare un numero preciso sia per quanto concerne la quantità di dati elaborati sia per il numero di persone interessate applicabile in tutte le situazioni. Il Gruppo di lavoro Articolo 29 raccomanda alcuni fattori da valutare per determinare se il trattamento è effettuato o meno su larga scala: numero di persone interessate, volute dei dati, durata ed estensione geografica dell'attività di trasformazione. Infine, le Linee Guida specificano che anche la nozione di monitoraggio regolare e sistematico delle persone interessate non è definita nel Regolamento, ma il concetto di «monitorare il comportamento delle persone interessate» è menzionato nel *considerando* 24 e comprende in modo chiaro tutte le forme di monitoraggio e profilazione su *Internet*, anche ai fini della pubblicità comportamentale. Come chiarito dalle FAQ in allegato alle Linee Guida del Gruppo di lavoro Articolo 29, per la protezione dei dati sono dunque tenuti alla nomina di un RPD, a titolo esemplificativo e non esaustivo: istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; sindacati; CAF e patronati; società operanti nel settore delle *utilities* (telecomunicazioni, distribuzione di energia elettrica o gas); imprese di somministrazione di

lavoro e ricerca del personale; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione; società di *call center*; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento. Non è obbligatoria la designazione del RPD nei casi diversi da quelli previsti dall'art. 37 paragrafo 1. Rimane comunque raccomandata su base volontaria la designazione di tale figura, in virtù del principio di responsabilizzazione. Il Gruppo di lavoro Articolo 29, nelle Linee Guida, incoraggia approcci di questo genere. La designazione non è invece obbligatoria, ad esempio, in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale; agenti, rappresentanti e mediatori operanti non su larga scala; imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti. La designazione di un unico RPD è prevista per più organismi. Il gruppo imprenditoriale (definizione n. 19 art. 4) può nominare un unico RPD a condizione che quest'ultimo sia facilmente raggiungibile da ciascuno stabilimento. È inoltre ammessa la designazione di un unico RPD per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione: si deve anche in questo caso assicurare la raggiungibilità del RPD. Il concetto di «raggiungibilità» è espresso al punto 2.3 delle Linee Guida del Gruppo Articolo 29 e si riferisce ai compiti del RPD in quanto punto di contatto. Il RPD deve essere in grado di comunicare in maniera efficace con gli interessati e di collaborare con le Autorità di controllo. Il Gruppo Articolo 29 ha indicato che i dati di contatto del RPD comprendono le informazioni che consentono agli interessati e all'Autorità di controllo di raggiungerlo facilmente. Il

ruolo in questione può essere ricoperto da un dipendente del titolare o del responsabile del trattamento che conosca la realtà operativa. La funzione di RPD può essere esercitata anche da persona giuridica esterna, a condizione che garantisca l'effettivo assolvimento dei compiti assegnati a tale figura dal Regolamento. Il RPD scelto all'interno è nominato mediante specifico atto di designazione, mentre la persona giuridica scelta all'esterno opera in base a un contratto di servizi. Gli atti, da redigere in forma scritta, devono indicare i compiti attribuiti, le risorse assegnate per il loro svolgimento e altre utili informazioni in rapporto al contesto di riferimento. Il ruolo di RPD è compatibile con altri incarichi, a condizione che non sia in conflitto di interessi. Il Gruppo Articolo 29 ha individuato buone prassi aziendali per far sì che non venga nominato un RPD in conflitto di interessi. È preferibile evitare di assegnare tale ruolo a soggetti con incarichi di alta direzione (es. amministratore delegato, direttore generale, ecc.), ovvero nell'ambito di strutture aventi potere decisionale in ordine alle modalità e finalità del trattamento. L'art. 37, al paragrafo 6, prevede che il RPD possa essere un dipendente del titolare o del responsabile del trattamento. Il RPD come persona fisica può anche essere supportato da un apposito ufficio dotato delle competenze necessarie ai fini dell'adempimento dei propri compiti. Qualora il RPD sia individuato in un soggetto esterno, quest'ultimo può anche essere una persona giuridica. È raccomandata una chiara ripartizione delle competenze, individuando una sola persona fisica che funga da punto di contatto con gli interessati e l'Autorità di controllo[270].

[270] In merito alla figura chiave del *Data Protection Officer* la letteratura è sterminata. Cfr. a tal proposito IASELLI M. (2018), *Manuale operativo del DPO (Data Protection Officer)*, Maggioli Editore, Santarcangelo di Romagna, che tenendo conto del recente decreto

### *4.3 Le misure di sicurezza e la notifica di violazione dei dati personali (data breach)*

Il titolare del trattamento, come pure il responsabile del trattamento, è obbligato ad adottare misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio del trattamento, con l'obiettivo di evitare distruzione accidentale o illecita, perdita, modifica, rivelazione, accesso non autorizzato. Fra tali misure, il Regolamento UE 2016/679 menziona, in particolare, la pseudonimizzazione e la cifratura dei dati; misure per garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; misure atte a garantire il tempestivo ripristino della disponibilità dei dati; procedure per verificare e valutare regolarmente l'efficacia delle misure di sicurezza adottate. La lista di cui al paragrafo 1 dell'articolo 32 è una lista aperta e non

---

legislativo n. 101/2018 di adeguamento della normativa nazionale al GDPR, approfondisce i compiti e le attività del DPO fornendo al lettore una guida operativa corredata da un formulario naturalmente orientativo in merito ai vari adempimenti da porre in essere; COMELLINI S. (2018), *Il responsabile della protezione dei dati (Data Protection Officer-DPO)*, Maggioli Editore, Santarcangelo di Romagna; MAIETTA A. (2020), *Il principio di autoresponsabilità. Il modello del Data Protection Officer*, G. Giappichelli Editore, Torino; per una lettura ragionata inerente alle dinamiche del ruolo del DPO, compresi i requisiti, le competenze e le attività sottostanti coinvolti nell'avvio o nello sviluppo di programmi sulla *privacy* e nella costruzione di una cultura che supporti la *privacy*, la sicurezza e l'integrità dei dati, cfr. JOHNSSÉN F., EDVARDSEN S. (2020), *Data Protection Officer,* BCS, The Chartered Institute for IT, Londra; si consiglia inoltre il volume di ACCIAI R., ANGELETTI S. (2019), *Il DPO protagonista dell'innovazione. Il responsabile della protezione dei dati tra competenze e certificazioni*, Aracne Editore, Roma, che esamina caratteristiche e compiti della nuova figura, alla luce anche delle *best practices* e dei percorsi di certificazione, tentando di fornire con spirito critico un'indicazione sul bagaglio tecnico che il DPO dovrebbe possedere e alimentare.

esaustiva ("tra le altre, se del caso"). Per questi motivi, non possono sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza[271] poiché tale valutazione è rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da articolo 32 del Regolamento. Il Regolamento prevede all'art. 32 alcune esemplificazioni di misure adeguate da adottare a seconda dei risultati dell'analisi dei rischi. I parametri sono i seguenti: stato dell'arte, costi di attuazione, natura, oggetto, contesto e finalità del trattamento, rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche. Le misure si classificano in tecniche e organizzative. La misura tecnica è affidata a una macchina, a un elaboratore. La conformità, quindi, dipende dalla correttezza della programmazione della macchina stessa. La misura organizzativa è affidata ai comportamenti delle persone, conformi a uno *standard* operativo. Secondo quanto disposto dal paragrafo 1 dell'art. 32, tra le misure sono comprese: 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

[271] Come sottolineato da FINOCCHIARO G. D. (2017), *Il quadro d'insieme*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, diretto da FINOCCHIARO G. D., Zanichelli, Bologna, p. 13, «la sicurezza è un concetto dinamico relazionale, rapportarsi alle conoscenze in base al progresso tecnico, alla natura dei dati personali oggetto di trattamento e dalle specifiche caratteristiche delle operazioni di trattamento compiute».

trattamento. Ai sensi del paragrafo 2 dell'art. 32, il livello di sicurezza è adeguato quando è in grado di contrastare rischi di distruzione, perdita, modifica, divulgazione non autorizzata, accesso in modo accidentale o illegale a dati personali trasmessi, conservati o comunque trattati. Il sistema di sicurezza viene realizzato mediante la formazione degli addetti al trattamento dei dati. Il Regolamento stabilisce che chiunque abbia accesso a dati personali può trattarli solo se è istruito il tal senso dal titolare del trattamento, salvo eccezioni di legge. Il paragrafo 3 dell'art. 32 prescrive che l'adesione a un codice di condotta o a un meccanismo di certificazione può dimostrare la conformità ai requisiti del paragrafo 1 dell'articolo in questione. L'art. 4 definisce la violazione dei dati personali[272] (definizione n. 12) come «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»[273]. Secondo

[272] Per un ampio contributo sul tema della violazione dei dati personali cfr. CUFFARO V., D'ORAZIO R., RICCIUTO V. (a cura di) (2019), *I dati personali nel diritto europeo*, G. Giappichelli Editore, Torino, p. 624 ss.; MAGLIO M., POLINI M., TILLI N. (2017), *Manuale di diritto alla protezione dei dati personali. La privacy dopo il Regolamento UE 2016/679*, Maggioli Editore, Santarcangelo di Romagna, in particolare la parte generale al punto 5.6 "*Data Breach Notification*: obbligo di notifica". Nella seconda edizione del volume (2019), si sono aggiunti capitoli che: esaminano il GDPR in rapporto con *Blockchain*, *Bitcoin*, *Data Protection* e Intelligenza Artificiale; illustrano il nuovo approccio delle misure di *Cybersecurity*, con profili pratico-operativi; propongono un'analisi compiuta di una casistica di *Data Breach*; affrontano i rapporti tra GDPR e D.Lgs. n. 231/2001, antiriciclaggio e misure di audit in campo *privacy*; offrono una più capillare analisi dell'applicazione dei principi di protezione dei dati personali veicolati nel *web*.

[273] Si tenga presente che i *security incidents* più ricorrenti statisticamente sono l'utilizzo abusivo di informazioni riservate, furto e

quanto disposto dall'art. 33 del Regolamento, in caso di violazione dei dati personali, i titolari del trattamento devono notificare la violazione all'Autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne sono venuti a conoscenza, ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà delle persone fisiche interessate (*considerando* 85). Pertanto, l'obbligo non scatta nel caso in cui il titolare del trattamento sia in grado di dimostrare che è improbabile che la violazione dei dati personali possa costituire un rischio. Qualora la notifica della violazione all'Autorità di controllo non sia effettuata entro 72 ore deve essere corredata dalle ragioni del ritardo. La notifica all'Autorità di controllo dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta al titolare del trattamento. Il paragrafo 3 dell'art. 33 stabilisce che la notifica di violazione deve almeno: a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione; b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni; c) descrivere le probabili conseguenze della violazione dei dati personali; d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per

perdita di dati, *crimeware* causati da *malware*, attacchi in generale perpetrati per mezzo di applicazioni *online*, accessi non autorizzati negli esercizi o attività commerciali in genere, errori, interruzioni di servizio, *skimming* e spionaggio informatico. Cfr. Articolo 29 Data Protection Working Party, *Working document 01 2011 on the current EU personal data breach framework and recommendations for future policy developments*, WP 184, adottato il 5 aprile 2011, p. 4 e ss.

porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi. Secondo quanto disposto dal paragrafo 5 dell'art. 33: «5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo». Ai sensi dell'art. 34 paragrafo 1, il titolare del trattamento deve comunicare all'interessato la violazione senza ingiustificato ritardo, al fine di consentirgli di prendere le precauzioni necessarie. La comunicazione all'interessato, secondo quanto dichiarato dal paragrafo 2, deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali; inoltre, deve contenere almeno le informazioni e le misure di cui all'art. 33, paragrafo 3, lettere b), c) e d). Il titolare del trattamento può decidere di non informare gli interessati se ritiene che la violazione non comporti un rischio elevato per i loro diritti (es. frode, furto di identità, danno di immagine); oppure se dimostrerà di avere adottato misure di sicurezza (come la cifratura) a tutela dei dati violati; oppure nell'eventualità in cui informare gli interessati può comportare uno sforzo sproporzionato (es. il numero delle persone coinvolte è elevato). Nel dettaglio, non è richiesta la comunicazione all'interessato (art. 34 paragrafo 3) se è soddisfatta una delle seguenti condizioni: a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura; b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui

al paragrafo 1; c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia. Conclude il paragrafo 4: «4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta»[274].

### *4.4 La valutazione d'impatto privacy (DPIA) e la consultazione preventiva*

La valutazione dei rischi[275] è sempre necessaria, come pure la sicurezza dei trattamenti. Nella valutazione dei rischi si deve tenere conto delle eventualità di distruzione accidentale o illegale, perdita, modifica, rivelazione o accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati. Bisogna tenere conto degli eventuali pregiudizi derivati: danni fisici, materiali o immateriali. È necessario elencare i rischi e catalogarli, poi

[274] Per maggiori delucidazioni in merito alla violazione di dati personali (*data breach*), in base alle previsioni del Regolamento (UE) 2016/679 si rinvia alle linee guida del Gruppo di lavoro "Articolo 29" disponibili *online* sul sito *web* del Garante per la protezione dei dati personali. Data di ultimo accesso e consultazione: 31 luglio 2020 (https://www.garanteprivacy.it/regolamentoue/databreach).

[275] MANTELERO A. (2017*), Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva (Artt. 32-39)*, in FINOCCHIARO G. D. (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, in particolare p. 301.

ordinarli[276]. Alla valutazione dei rischi segue la valutazione di impatto che, ai sensi dell'art. 35, è una attività riservata ai «rischi elevati» e presuppone il coinvolgimento dell'Autorità Garante. È anche chiamata *Privacy Impact Assessment* (PIA) oppure, in alternativa, *Data Protection Impact Assessment* (DPIA)[277]. La valutazione d'impatto sulla protezione dei dati va effettuata prima del trattamento. I Garanti della *privacy* a livello europeo (Articolo 29), nelle Linee Guida in materia di valutazione di impatto *privacy* emanate il 4 ottobre 2017, affermano che la DPIA è necessaria anche per i trattamenti che sono già in corso[278]. Mediante questa attività si acquisiscono le necessarie conoscenze sulle misure, sulle garanzie e sui meccanismi previsti per attenuare il rischio e assicurare la conformità del trattamento agli *standard*. Così recita il paragrafo 2 dell'art. 35: «2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati,

[276] BERNARDI N., CICCIA MESSINA A. (2017), *Privacy e Regolamento Europeo*, IPSOA, Milano, p. 112 ss.

[277] DI RESTA F. (2018), *La nuova «privacy europea». I principali adempimenti del regolamento UE 2016/679 e profili risarcitori*, G. Giappichelli Editore, Torino, p. 125 ss. Nel volume è dedicata particolare importanza al nuovo approccio proattivo all'analisi dei rischi e alla valutazione di impatto (DPIA), che, secondo l'autore, insieme al registro delle attività di trattamento e alla violazione dei dati personali (*data breach*) costituiscono l'architrave della nuova "*privacy* europea"; MAGLIO M., POLINI M., TILLI N. (2017), op. cit., in particolare la parte generale al punto 5.9 "*Data protection impact assessment o PIA: analisi e gestione dei rischi*".

[278] Per maggiori delucidazioni in merito alla valutazione d'impatto sulla protezione dei dati si rinvia alle linee guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati (WP248) disponibili *online* sul sito *web* del Garante per la protezione dei dati personali. Data di ultimo accesso e consultazione: 28 luglio 2020. (https://www.garanteprivacy.it/valutazione-d-impatto-della-protezione-dei-dati-dpia-).

qualora ne sia designato uno». Il paragrafo 3 stabilisce che la valutazione d'impatto sulla protezione dati è richiesta in particolare nei seguenti casi: a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico. Ai paragrafi 4 e 5 il Regolamento assegna all'Autorità Garante il compito di redigere e rendere pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto e anche un elenco delle tipologie di trattamenti per le quali non è richiesta. La valutazione d'impatto contiene almeno (art. 35, paragrafo 7): a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione. Nel valutare l'impatto del trattamento bisogna rispettare i codici di condotta (art. 35 paragrafo 8). Il Regolamento prevede che il titolare effettui il costante monitoraggio dei trattamenti in relazione a eventuali variazioni del rischio per la protezione dei dati (art. 35 paragrafo 11). L'esito

della valutazione d'impatto può essere favorevole o negativo. Nel primo caso, dunque, è possibile iniziare il trattamento; nel secondo potrebbe scaturire il mancato avvio del trattamento oppure potrebbe avviarsi una procedura che interessa l'Autorità di controllo[279]. La mancata esecuzione della DPIA nei casi di obbligatorietà o l'errata valutazione possono comportare l'applicazione di una sanzione pari nel massimo a 10 milioni di euro oppure, nel caso dell'impresa, fino a 2% del fatturato globale dell'anno precedente, in base a quale dei due importi sia quello superiore (art. 83, paragrafo 4, lettera a) del Regolamento 2016/679). In taluni casi la valutazione d'impatto *privacy* non basta ed è opportuno consultare preventivamente l'Autorità Garante (art. 36). Se dalla valutazione d'impatto emergesse che il rischio per la protezione dei dati non potesse essere ragionevolmente attenuato mediante l'uso delle tecnologie disponibili e per gli elevati costi di attuazione, è necessario consultare l'Autorità di controllo prima dell'inizio delle attività di trattamento. La richiesta di consultazione, secondo quanto disposto dall'art. 36 paragrafo 3, contiene: a) ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale; b) le

[279] TSIOURAS I. (2020), *GDPR. Privacy Risk Management*, Youcanprint, Lecce. Il presente volume riprende passo i concetti delle norme, sviluppa le prescrizioni e gli approcci ed entra in dettaglio nei concetti approfondendo con esempi pratici e dettagliati il processo di *Privacy Risk Management*. Precisa giustamente l'autore che la norma ISO/IEC 27701 è stata emessa per aiutare le organizzazioni a far fronte alla difficoltà che riscontrano per soddisfare il requisito dell'art. 35 del GDPR relativo alla valutazione d'impatto dei trattamenti previsti sulla protezione dei dati personali. La norma specifica i requisiti in una forma che si estende alla ISO/IEC 27001, ISO/IEC 27002, ISO 27018 e la serie ISO/IEC 29000 per la gestione della *privacy*.

finalità e i mezzi del trattamento previsto; c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento; d) ove applicabile, i dati di contatto del titolare della protezione dei dati; e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35; f) ogni altra informazione richiesta dall'autorità di controllo. La richiesta di consultazione contiene la valutazione d'impatto: non è possibile fare una richiesta di consultazione senza aver prima completato la valutazione d'impatto. In questo contesto, il trattamento in questione mette a rischio la protezione delle persone fisiche. Ai sensi del paragrafo 2 dell'art. 36, se ritiene che il trattamento violi il Regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'Autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'art. 58. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'Autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'Autorità di controllo delle informazioni richieste ai fini della consultazione.

### *4.5 Le tecniche di protezione dati privacy by design e privacy by default*

Il *General Data Protection Regulation* (GDPR) introduce il concetto di *Privacy by Design* e *Privacy by Default*. Si tratta di 2 modalità di gestione della protezione[280], disciplinate all'art. 25 del GDPR, cioè dopo la definizione generale del ruolo di titolare del trattamento, in quanto profili della sua responsabilizzazione. L'art. 25 è centrale poiché fa riferimento sia all'istituto della protezione dei dati «fin dalla progettazione» (*Privacy by design*), che a quello della protezione dei dati «per impostazione predefinita» (*Privacy by default*). Vengono individuati 7 princìpi[281] su cui si fonda la *Privacy by design* e by *default*:

[280] CICCIA MESSINA A., BERNARDI N. (2017), *Privacy e Regolamento Europeo*, IPSOA, Milano, p. 85 ss.; PIZZETTI F. (2016), *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, G. Giappichelli Editore, Torino, p. 45 ss.

[281] PAGANO R. (2017), *L'organizzazione aziendale per l'implementazione del Sistema Privacy. Tutti i passi utili all'adozione di un sistema privacy conforme alle norme vigenti*, Independently published, p. 31. Secondo l'autore, al fine di poter essere conformi con le norme vigenti sulla *privacy* le organizzazioni devono implementare un sistema capace di sovraintendere i processi relativi alla protezione dei dati nonché garantire la conformità alle norme in vigore. L'approccio con cui viene realizzato un Sistema *Privacy* è mutuato dal sistema di gestione della qualità basato sulle norme della famiglia ISO 9000 con un indirizzo orientato verso il miglioramento ed alla integrazione con altri sistemi di gestione come, per esempio, la UNI EN ISO 27001:2013 relativo ai sistemi di gestione della sicurezza delle informazioni. Il Sistema *Ius Privacy* prevede l'adozione delle regole di *Enterprise Risk Management* cioè l'insieme delle attività mirate a individuare, valutare, gestire e controllare tutti i tipi di eventi (rischi) a cui sono soggetti gli *asset* dell'organizzazione: beni materiali, beni immateriali, documentali. Obiettivi del *Sistema Privacy*: - Garantire la conformità alle norme vigenti in materia (Codice *Privacy*, Provvedimento del Garante, Regolamento Europeo); - Stabilire le

1. Prevenire e non correggere: i problemi vanno valutati nella fase di progettazione; 2. *Privacy* come impostazione di default; 3. *Privacy* incorporata nel progetto; 4. Massima funzionalità, in maniera da rispettare tutte le esigenze; 5. Sicurezza durante tutto il ciclo del prodotto o servizio; 6. Trasparenza; 7. Centralità dell'utente. Secondo questo orientamento il sistema *privacy* deve essere *user centric*, cioè è l'utente che è al centro dell'intero sistema, non è più sufficiente una progettazione che sia conforme a norma se poi l'utente non è adeguatamente protetto. Il paragrafo 1 dell'art. 25 del Regolamento Europeo enuncia l'obbligo della *Privacy by Design* rivolta ai titolari del trattamento: «1. 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». Il principio in questione obbliga il titolare, nel momento in cui determina finalità e modalità del trattamento, tenuto conto dei rischi del trattamento stesso, dello stato dell'arte delle tecnologie e dell'ambito di applicazione, di mettere in atto misure tecniche e organizzative adeguate a integrare nel trattamento le necessarie garanzie per tutelare i diritti degli interessati. Integrare le tutele nel trattamento. È

procedure da seguire per proteggere i dati; - Come risultato derivato dalla *compliance*, proteggere i dati aziendali, l'immagine e la reputazione aziendale.

questo il passaggio chiave, al quale due significati possono essere attribuiti: o trattare i dati in modo da minimizzarne l'uso per perseguire una finalità, al punto da non ritenersi più necessario un trattamento di dati personali, ovvero trattarli in modo da incrementarne la sicurezza, rafforzando la confidenzialità del dato. In altre parole, significa ridurre al minimo il trattamento dei dati personali, adottando misure tecniche e organizzative, come ad esempio la pseudonimizzazione, la quale consiste nel sostituire un attributo, solitamente univoco, di un dato con un altro, ugualmente univoco e solitamente non immediatamente intellegibile. Questo accorgimento può rendere più complessa l'identificazione, richiedendo mezzi anche onerosi per la riferibilità del dato alla persona, ma mantiene inalterato il quadro di certezze nella concatenazione dei passaggi necessari per l'attribuzione del dato pseudonimo della persona. La *Privacy by Design* si presenta come approccio molto appropriato per un contesto *data intensive* come quello dei *big data*[282] e rappresenta il futuro della *privacy*: ancor prima di iniziare il trattamento e la raccolta

[282] Cfr. MANTELERO A. (2018), *La privacy all'epoca dei big data*, in *Protezione e libera circolazione dei dati personali nel diritto europeo. Il regolamento generale 2016/679 (e le direttive 2016 680 e 2016 681 sul trattamento dei dati in ambito penalistico)*, CUFFARO V., D'ORAZIO R., RICCIUTO V. (a cura di), G. Giappichelli Editore, Torino; GRUSCHKA N., MAVROEIDIS V., VISHI K., JENSEN M. (2018), *Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR*, IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, pp. 5027-5033. Il *paper* presenta le implicazioni del GDPR su progetti che si avvalgono dei *big data*. Mediante due casi studio, gli autori hanno analizzato come possono essere applicate le tecniche di tutela della *privacy*. È di grande importanza osservare che per progetti e tecnologie che trattano dati sensibili, la valutazione d'impatto sulla protezione dei dati dovrebbe essere condotta durante le primissime fasi del progetto per identificare la potenziale *privacy challenges* e adattare i metodi di analisi prendendo in considerazione le tecniche di *privacy preserving*.

dati, le organizzazioni dovranno effettuare una *Privacy Impact Assessment* (PIA). Quest'ultima sarà effettuata dal DPO designato dall'organizzazione che valuterà le misure e gli accorgimenti da suggerire all'azienda[283]. Il paragrafo 2 dell'art. 25 fa riferimento alla *Privacy by Default*: «2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per 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». Concerne la protezione dei dati per impostazione predefinita e impone dunque al titolare di adottare le misure tecniche necessarie a garantire che siano trattati solo i dati necessari rispetto alla finalità del trattamento. Il titolare deve assicurare, fin dalla fase della progettazione dei trattamenti, che anche «la quantità dei dati raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità» siano solo quelli strettamente necessari rispetto alle finalità. Deve garantire

[283] Per un approfondimento sul tema della pseudonimizzazione e anonimizzazione cfr. D'ACQUISTO G., NALDI M. (2017), *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, G. Giappichelli Editore, Torino, in particolare p. 41 ss., p. 117 ss. Il volume si pone l'obiettivo di illustrare le principali modalità disponibili per offrire alle persone nuove tutele basate sulla leva tecnologica in aggiunta a quelle che tradizionalmente si sono realizzate intervenendo sulla leva giuridica, mediante l'adozione di processi di anonimizzazione e pseudonimizzazione dei dati. Secondo gli autori, op. cit., se diritto e tecnologia saranno ben armonizzati, la maggiore disponibilità di dati potrà realmente determinare un cambiamento di tipo cognitivo, permettendoci la scoperta di nuove relazioni tra dati (i *big data*), le persone e gli oggetti (l'*internet* delle cose).

infine che non siano resi accessibili in modo automatico dati personali riferibili a un numero indefinito di persone fisiche[284].

### *4.6 Codici di condotta e meccanismi di certificazione*

Una importante novità introdotta dal Regolamento 2016/679 è la previsione di codici di condotta e di meccanismi di certificazione che consentano agli interessati di valutare il livello di protezione dei dati dei relativi prodotti e servizi, migliorando trasparenza e il rispetto dello stesso Regolamento. Sono strumenti che incidono sulla responsabilità del *controller* (e, per quanto di sua competenza del *processor*): la loro adozione può concorrere a dimostrare la loro volontà di *compliance* rispetto ai loro doveri. Da questo punto di vista il Regolamento costituisce una novità significativa rispetto alla Direttiva 95/46, non solo perché in quella sono previsti solo i codici di condotta e non le certificazioni, ma anche perché i codici di condotta non hanno, nella Direttiva, una incidenza immediata sulla responsabilità del titolare e del responsabile, se non nel senso che la loro adozione vincola questi a rispettare non solo le norme della Direttiva ma anche i vincoli che i codici di condotta contengono in

[284] Per ulteriore approfondimento cfr. i volumi di BINCOLETTO G. (2019), *La privacy by design. Un'analisi comparata nell'era digitale*, Aracne Editrice, Roma; BASSANI M., BIFULCO R., D'ACQUISTO G., NALDI M., POLLICINO O., PIZZETTI F. (a cura di) (2018), *Intelligenza artificiale, protezione dei dati personali e regolazione,* G. Giappichelli Editore, Torino. Per una accurata analisi con particolare riferimento all'*Internet of Things* (IoT) cfr. ALJERAISY A., RANA O., PERERA C. (2020), *A Systematic Analysis of Privacy Laws and Privacy by Design Schemes for the Internet of Things: A Developer's Perspective*, HAL archives ouvertes, Pré-publication.

ordine alla loro interpretazione e attuazione. È dunque giusto segnalare la stretta connessione tra questi strumenti e il principio di responsabilità come declinato nel Regolamento[285]. Secondo quanto disposto dall'art. 40, gli Stati membri, le Autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del Regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese. Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione del Regolamento, ad esempio relativamente a: a) il trattamento corretto e trasparente dei dati; b) legittimi interessi perseguiti dal responsabile del trattamento in contesti specifici; c) la raccolta dei dati personali; d) la pseudonimizzazione dei dati personali; e) l'informazione fornita al pubblico e agli interessati; f) l'esercizio dei diritti degli interessati; g) l'informazione fornita e la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore; h) le misure e le procedure sul *privacy by design* e sulle modalità di sicurezza; i) la notifica di una violazione dei dati personali alle Autorità di controllo e la comunicazione di tali violazioni dei dati personali dell'interessato; j) il trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali; k) le procedure stragiudiziali e di altro tipo per comporre le controversie tra titolari del trattamento e interessati in materia del trattamento. Le associazioni e gli altri organismi che intendono elaborare

[285] PIZZETTI F. (2016), *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, G. Giappichelli Editore, Torino, pp. 300 – 301.

un codice di condotta o modificare o prorogare un codice esistente sottopongono il progetto di codice, la modifica o la proroga all'Autorità di controllo competente. L'Autorità di controllo esprime un parere sulla conformità al Regolamento del progetto di codice, della modifica o della proroga e se ritiene che offra in misura sufficiente garanzie adeguate dà l'approvazione registrando e pubblicando il codice. La certificazione è prevista e regolata dall'art. 42 del Regolamento Europeo[286]. Può essere rilasciata dagli organismi di certificazione di cui all'art. 43 o dall'Autorità di controllo competente a un titolare del trattamento o a un responsabile del trattamento per un periodo massimo di 3 anni; può essere rinnovata alle stesse condizioni purché continuino a essere soddisfatti i requisiti pertinenti. Qualora non siano soddisfatti i requisiti, la certificazione può essere revocata dagli organismi di certificazione o dall'Autorità di controllo competente. La certificazione non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità del Regolamento e lascia impregiudicati i compiti e poteri delle Autorità di controllo competenti[287]. Il Comitato

[286] A livello europeo cfr. EDPB, *Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation 2016/679*, adottate il 4 dicembre 2018. Ultima consultazione all'indirizzo https://edpb.europa.eu/ in data 15 luglio 2020. Le linee guida sono volte a stabilire criteri per l'accreditamento degli enti certificatori, ossia quegli enti che possono rilasciare certificazioni di cui all'art. 42 del GDPR.

[287] L'enfasi in merito alle certificazioni è espressa anche da PIVA A., FERRI S., SALA M. (2019), *Privacy alla luce del Regolamento Europeo UE 2016/679. Guida alla certificazione «Protezione dati personali: GDPR, Privacy e Sicurezza»*, A.I.C.A. Editore. Il volume è inoltre un utile riferimento e guida per la preparazione alla certificazione AICA "Protezione dati personali: GDPR, Privacy e Sicurezza". Per una ulteriore lettura in merito ai codici di condotta e ai meccanismi di certificazione cfr. PANETTA R. (2019), *Il trasferimento all'estero dei dati*

europeo per la protezione dei dati raccoglie in un registro tutti i meccanismi di certificazione e i sigilli e i marchi di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato[288].

### *4.7 Il trasferimento di dati verso Paesi terzi*

La circolazione dati[289], oggetto specifico della disciplina del Regolamento 2016/679, può avvenire in ambiti coperti dall'ambito di applicazione del Regolamento stesso oppure verso ambiti non coperti. Quando ricorre quest'ultima evenienza si tratta di trasferimento di dati all'estero, una tipologia di trattamento dati pericoloso per le persone fisiche cui si riferisce. All'art. 44 è sancito il «principio generale per il trasferimento», secondo cui qualunque trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale è legittimo solo se il titolare e il responsabile del trattamento rispettano le condizioni previste dal Regolamento. La pretesa egemonica dell'Unione Europea sulla tutela dei dati personali[290] trova dunque proprio nell'art. 44 la sua massima affermazione. L'articolo sottolinea la centralità che il flusso di dati personali (verso e da Paesi terzi e

---

*personali*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, (a cura di) ZORZI GALGANO N., Cedam, Padova, in particolare al paragrafo 7, pp. 370-372.

[288] BERNARDI N., CICCIA MESSINA A. (2017), *Privacy e Regolamento Europeo*, IPSOA, Milano, p. 129

[289] L'enfasi sulla libertà di circolazione è espressa da: SICA S. (2016), *Verso l'unificazione del diritto europeo alla tutela dei dati personali?*, in *La nuova disciplina europea della privacy*, SICA S., D'ANTONIO V., RICCIO G. M. (a cura di), Cedam, Padova, p. 2 ss.

[290] PIZZETTI F. (2016), *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, G. Giappichelli Editore, Torino, p. 89.

organizzazioni internazionali) ha assunto nella società contemporanea. Sono previste tre situazioni ordinarie e alcune straordinarie nelle quali è possibile trasferire i dati verso Paesi terzi[291]. Al di fuori di tali situazioni ordinarie ed eccezionali, il trasferimento dei dati personali verso Paesi terzi non è mai consentito. 1. Dichiarazione di adeguatezza della Commissione europea (*adequacy*). Nel primo caso, la Commissione europea nella valutazione di adeguatezza prende in considerazione precisi elementi espressamente previsti dall'art. 45 paragrafo 2 del Regolamento 2016/679. Successivamente viene svolto un riesame periodico di tale decisione (almeno ogni quattro anni), al fine di mantenere sotto osservazione l'effettiva esistenza di un adeguato livello di protezione, in conformità con quanto previsto dal GDPR. Le decisioni della Commissione europea devono essere pubblicate nella Gazzetta Ufficiale dell'Unione Europea e sul sito della Commissione europea stessa. Una volta riconosciuto adeguato un determinato Paese, tutti i trasferimenti verso quest'ultimo non devono più ottenere autorizzazioni

[291] Cfr. sul tema del trasferimento dati verso Paesi terzi MAGLIO M., POLINI M., TILLI N. (2017), *Manuale di diritto alla protezione dei dati personali. La privacy dopo il Regolamento UE 2016/679*, Maggioli Editore, Santarcangelo di Romagna (RN), in particolare cap. 7; cfr. anche FABIANO N. (2020), *GDPR & Privacy: consapevolezza e opportunità. L'approccio con il Data Protection and Privacy Relationships Model (DAPPREMO)*, goWare, Firenze. Nel volume viene presentato un nuovo e innovativo approccio alla protezione dei dati secondo il modello relazionale che è stato definito DAPPREMO (acronimo di *Data Protection and Privacy Relationships Model*) basato sulla matematica in funzione dell'analisi della realtà. Le nuove frontiere tecnologiche (*blockchain*, IoT, *big data*, intelligenza artificiale, droni, robotica) meritano attenzione soprattutto in considerazione dell'impatto sulla protezione dei dati personali; è sempre più necessaria adeguata consapevolezza anche al fine di un corretto approccio etico al tema.

specifiche di alcun tipo (art. 45). 2. Il trasferimento soggetto a garanzie adeguate. Nel secondo caso, ai sensi dell'art. 46, il titolare o il responsabile del trattamento può trasferire i dati personali verso un Paese terzo solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi. Alcune garanzie adeguate che vengono elencate dal Regolamento sono: norme vincolanti di impresa, clausole contrattuali *standard* adottate dalla Commissione o dalle Autorità di controllo, codici di condotta o certificazioni. 3. Trasferimento dei dati e norme vincolanti d'impresa (BCR – *Binding Corporate Rules*). Il terzo caso riguarda una procedura volta a consentire il trasferimento verso Paesi *extra* UE tra società facenti parte dello stesso gruppo d'impresa. Previste dall'art. 47, consistono in una serie di clausole contrattuali che dettano principi vincolanti per tutte le società facenti parte del gruppo. L'art. 47 non definisce il concetto di norme vincolanti d'impresa, rinviando a questo fine all'art. 4, che ne contiene la definizione, al numero 20 del paragrafo 1. Le *Binding Corporate Rules* vengono esaminate e approvate dall'Autorità di controllo nazionale o europea, la quale verifica la sussistenza dei contenuti minimi previsti dall'art. 47 del Regolamento. 4. Altri casi di legittimo trasferimento dati all'estero. Oltre alle tre situazioni ordinarie sopraccitate, esistono deroghe previste dal legislatore europeo. Il trasferimento è ammesso solo se l'interessato ha espressamente ed esplicitamente consentito al trasferimento, dopo essere stato informato dei possibili rischi e del fatto che il trasferimento stesso non rientra in nessuna delle situazioni ordinarie, o quando tale trasferimento è necessario per l'esecuzione di un contratto a favore dell'interessato o per importanti motivi di ordine pubblico, interessi vitali o per accertare, esercitare o difendere un diritto in sede giudiziaria. Il trasferimento

verso Paesi *extra* UE è ammesso solo se non è ripetitivo, riguarda un numero limitato di interessati ed è necessario per il perseguimento di interessi legittimi cogenti del titolare del trattamento, su cui non prevalgono gli interessi o i diritti e le libertà dell'interessato, e qualora il titolare del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali[292]. Il titolare informa comunque l'Autorità di controllo e, oltre alla solita informativa, mette a

[292] Cfr. Considerando 102: «Il presente regolamento lascia impregiudicate le disposizioni degli accordi internazionali conclusi tra l'Unione e i paesi terzi che disciplinano il trasferimento di dati personali, comprese adeguate garanzie per gli interessati. Gli Stati membri possono concludere accordi internazionali che implicano il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali, purché tali accordi non incidano sul presente regolamento o su qualsiasi altra disposizione del diritto dell'Unione e includano un adeguato livello di protezione per i diritti fondamentali degli interessati» e Considerando 115: «Alcuni paesi terzi adottano leggi, regolamenti e altri atti normativi finalizzati a disciplinare direttamente le attività di trattamento di persone fisiche e giuridiche poste sotto la giurisdizione degli Stati membri. Essi possono includere le sentenze di autorità giurisdizionali o le decisioni di autorità amministrative di paesi terzi che dispongono il trasferimento o la comunicazione di dati personali da parte di un titolare del trattamento o di un responsabile del trattamento e non sono basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro, ad esempio un trattato di mutua assistenza giudiziaria. L'applicazione extraterritoriale di tali leggi, regolamenti e altri atti normativi potrebbe essere contraria al diritto internazionale e ostacolare il conseguimento della protezione delle persone fisiche assicurata nell'Unione con il presente regolamento. I trasferimenti dovrebbero quindi essere consentiti solo se ricorrono le condizioni previste dal presente regolamento per i trasferimenti a paesi terzi. Ciò vale, tra l'altro, quando la comunicazione è necessaria per un rilevante motivo di interesse pubblico riconosciuto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento».

conoscenza l'interessato del trasferimento e degli interessi legittimi cogenti perseguiti (art. 49).

### *4.8 L'inasprimento della responsabilità e del sistema sanzionatorio*

Ai sensi dell'art. 78, l'interessato gode di tutela amministrativa e giurisdizionale. L'interessato ha diritto di proporre un ricorso giurisdizionale effettivo per la tutela dei propri diritti. In tal caso, sono competenti le Autorità giurisdizionali dello Stato membro in cui il titolare o il responsabile del trattamento ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle Autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente, salvo che il titolare o il responsabile del trattamento sia un'Autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri (artt. 78 – 79). Qualora l'interessato si ritenga leso nelle sue prerogative ha diritto di proporre un reclamo a un'Autorità Garante, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure del luogo nel quale si è verificata la presunta violazione. È fatto salvo ogni altro ricorso amministrativo o giurisdizionale (art. 77 paragrafo 1). L'Autorità Garante informa il reclamante dello Stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale, contro gli atti che definiscono il reclamo (art. 77 paragrafo 2). Rispetto all'impianto del Codice in materia di protezione dei dati personali, il Regolamento Europeo 2016/679 non ripropone espressamente la triade «segnalazione, reclamo e ricorso», limitandosi a disciplinare nelle procedure a disposizione dell'interessato riguardanti il Garante il reclamo, che equivale al ricorso. Con il nuovo Regolamento il contenzioso vero e proprio è promosso con un atto chiamato «reclamo» e non più

«ricorso». Il termine «ricorso» è riservato dal Regolamento al contenzioso portato dall'interessato contro un titolare del trattamento davanti al giudice ordinario[293]. Il «diritto al risarcimento e responsabilità»[294] è previsto dall'art. 82 del Regolamento 2016/679. Il paragrafo 1 enuncia la seguente dichiarazione: «Chiunque subisca un danno materiale o immateriale causato da una violazione del presente Regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento». Dunque, il paragrafo 1 dell'art. 82: 1. enuncia il diritto a ottenere il risarcimento del danno patrimoniale e non patrimoniale; 2. precisa la tipicità della condotta: occorre inquadrare l'atto o l'omissione illecita quale violazione di una prescrizione del Regolamento; 3. elenca i soggetti tenuti al risarcimento. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno devono essere promosse dinanzi alle Autorità giurisdizionali competenti a norma del diritto dello Stato membro. Secondo quanto disposto dall'art. 83, in materia di sanzioni amministrative l'Autorità di controllo esercita il potere di ingiungere il pagamento di una somma di denaro. Lo scopo delle sanzioni è sia repressivo (reprimere passati illeciti) che preventivo (prevenire illeciti futuri). Con l'introduzione del nuovo Regolamento, il sistema sanzionatorio è stato innovato nei seguenti ambiti[295]: a)

---

[293] CICCIA MESSINA A., BERNARDI N. (2017), *Privacy e Regolamento Europeo*, IPSOA, Milano, p. 144 ss.

[294] TOSI E. (2019), *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale. Oggettivazione del rischio e riemersione del danno morale con funzione deterrente-sanzionatoria alla luce dell'art. 82 GDPR*, Giuffrè Editore, Milano.

[295] CICCIA MESSINA A. (2016), *Regolamento Privacy UE: pro e contro del nuovo sistema sanzionatorio*, Rapporto di lavoro in IPSOA Quotidiano, pp. 1-3. Disponibile *online* al seguente indirizzo *world wide web*: https://www.ipsoa.it/documents/lavoro-e-previdenza/rapporto-di-lavoro/quotidiano/2016/10/19/regolamento-privacy-ue-pro-e-contro-

innalzamento dell'importo delle sanzioni; b) alternatività sanzioni pecuniarie e ammonizione; c) inserimento della violazione di tutti i principi e di tutti gli obblighi tra gli illeciti amministrativi. La declaratoria generale stabilisce che le sanzioni amministrative devono essere in concreto effettive, proporzionate e dissuasive. L'Autorità Garante può decidere nei singoli casi se applicare o meno le sanzioni amministrative pecuniarie in aggiunta alle misure di carattere prescrittivo o interdittivo. Ad esempio, se la sanzione pecuniaria imposta costituisse un onere sproporzionato per la persona fisica, potrebbe essere rivolto un ammonimento anziché la sanzione pecuniaria. Il paragrafo 2 dell'art. 83 elenca gli elementi da valutare nella decisione, in relazione all'ammontare della sanzione. Il nuovo sistema sanzionatorio prevede due fasce: la prima fascia ha come massimo edittale l'importo di 10 milioni di euro, mentre la seconda fascia 20 milioni di euro. Tali cifre possono ulteriormente incrementarsi per le imprese, se si applica la sanzione in misura percentuale, pari rispettivamente al 2% o al 4% del fatturato mondiale globale annuo. La misura percentuale si applica nel caso in cui sia superiore alla misura fissa. La prima fascia si applica alla violazione degli obblighi: 1. del titolare e del responsabile (artt. 8, 11, da 25 a 39, 42 e 43); 2. dell'organismo di certificazione (artt. 42 e 43); 3. dell'organismo di controllo (art. 41, paragrafo 4). La seconda fascia si applica in caso di violazione dei: 1. principi di base del trattamento, comprese le condizioni relative al consenso (artt. 5, 6, 7 e 9); 2. diritti degli

---

del-nuovo-sistema-sanzionatorio. Data di ultima consultazione: 5 luglio 2020. Le sanzioni amministrative previste dal regolamento europeo sulla *privacy* danno più spazio d'azione ai Garanti: nelle ipotesi lievi possono limitarsi a un ammonimento, senza strascichi pecuniari. Il Regolamento prevede che circa la metà delle prescrizioni sia assistita da sanzioni amministrative.

interessati (artt. da 12 a 22); 3. trasferimenti di dati personali *extra* UE (artt. da 44 a 49); 4. obblighi previsti dagli Stati nelle materie del Capo IX (artt. da 85 a 91, ad esempio giornalismo, lavoro, ricerca scientifica, storica, statistica, segreto professionale); 5. inosservanza di un ordine o di una limitazione del Garante o il negato accesso ai dati e ai locali (art. 58, c. 1 e 2). Per ciò che concerne le sanzioni penali, è concesso agli Stati membri stabilire disposizioni per eventuali violazioni del Regolamento (art. 84). Le sanzioni in questione possono autorizzare la sottrazione dei profili ottenuti attraverso violazioni del Regolamento. L'imposizione di sanzioni penali per violazioni di norme nazionali e sanzioni amministrative non può essere in contrasto col principio interpretato dalla Corte di Giustizia del *ne bis in idem*, locuzione latina che tradotta alla lettera significa «non due volte per la medesima cosa»[296].

[296] In merito al sistema sanzionatorio cfr. IASELLI M. (2019), *Sanzioni e responsabilità in ambito GDPR*, Giuffrè Editore, Milano. Il volume, privilegiando un approccio di carattere operativo, approfondisce le conseguenze derivanti dalla violazione in materia di protezione dei dati personali in termini di sanzioni e responsabilità. Vengono dapprima esaminati i diversi diritti dell'interessato, prendendo come punto di riferimento le illuminanti linee guida dei Garanti europei. Successivamente si approfondiscono le caratteristiche del controllo ispettivo alla luce della nuova normativa comunitaria e nazionale, analizzando i criteri di applicazione delle sanzioni amministrative pecuniarie e degli illeciti penali vigenti, in particolare, nel nostro ordinamento.

# SEZIONE SECONDA

## LA CERTIFICAZIONE ISO/IEC 27701:2019

## E L'IMPLEMENTAZIONE DEL

## PRIVACY INFORMATION MANAGEMENT SYSTEM

# CAPITOLO 4

# PRIVACY INFORMATION MANAGEMENT SYSTEM

**SOMMARIO:** 1. Introduzione – 2. La necessità di uno standard sulla protezione dei dati personali – 3. Il livello di accountability: responsabilità e fiducia nel trattamento delle informazioni personali – 4. Lo standard internazionale per la gestione delle informazioni sulla privacy ISO 27701: lo strumento pratico per la compliance al GDPR – 5. Realizzare il Privacy Information Management System – 6. Audit e controlli – 7. Certificazione e accreditamento.

## 1. Introduzione

Con l'aumento delle minacce e delle conseguenze derivanti da pratiche inadeguate sulla *privacy*, vi è un crescente interesse per la protezione dei dati personali e delle informazioni di identificazione personale (PII). Nonostante il crescente regime normativo sulla *privacy* a livello globale, non esiste un modo universalmente riconosciuto per ottenere la totale conformità (*compliance*) o dimostrare che un'organizzazione può essere considerata attendibile per il proprio approccio alla *privacy*. L'Organizzazione internazionale per la standardizzazione (ISO) ha rilasciato le tecniche di sicurezza ISO / IEC 27701: 2019 per la gestione delle informazioni sulla *privacy* con la conseguente crescita di quello che sta diventando noto come *Privacy Information Management Systems* (PIMS).

Le organizzazioni si stanno adeguando sempre più all'approccio congiunto di estendere a un sistema esistente di gestione della sicurezza delle informazioni (ISMS) certificato ISO 27001 la ISO 27701:2019 per approfondire ulteriormente i processi e i controlli sulla *privacy* che interessano i dati personali. È uno degli *standard* più attesi in sicurezza delle informazioni e gestione della *privacy* con lo scopo di colmare il divario di garanzia e fornire un approccio internazionale alla protezione dei dati come estensione alla sicurezza delle informazioni. Le organizzazioni con il desiderio di affrontare le sfide della conformità in materia di sicurezza delle informazioni e protezione dei dati possono trarre considerevoli vantaggi dall'implementazione della nuova normativa. Lo *standard* illustra un *set* completo di controlli operativi che può essere mappato alle diverse normative internazionali, incluso il GDPR. Dopo aver eseguito il *mapping*, i controlli operativi PIMS vengono implementati da professionisti della *privacy* e controllati da revisori interni o da terze parti, con conseguente certificazione e prova della conformità. L'articolo 42 del GDPR discute i requisiti di certificazione della protezione dei dati ma non esistono ancora tali meccanismi in quanto in via di definizione a livello europeo, sebbene la ISO 27701 sia ora formalmente stabilita. Tuttavia, è possibile ottenere una certificazione accreditata in modo indipendente secondo ISO 27001 - e per estensione ISO 27701 se si implementano i suoi controlli - che dimostrerà agli *stakeholder* e alle autorità di regolamentazione che la propria organizzazione sta seguendo le migliori pratiche internazionali quando si tratta di proteggere i dati personali.

## 2. La necessità di uno standard sulla protezione dei dati personali

Il drammatico aumento degli attacchi informatici alle imprese, indipendentemente dalle dimensioni, ha spinto il panorama della sicurezza e della *privacy* a diventare sempre più regolamentato. Le informazioni di base e la *privacy* dei dati sono al centro delle stringenti normative di sicurezza. Lo testimoniano le normative sulla *privacy* introdotte negli ultimi anni, come il GDPR, il DPA (Data Protection Act) del Regno Unito e il CCPA (*California Consumer Privacy Act*). Non da meno, le ammende che ricevono le organizzazioni non conformi a questi requisiti legali e che subiscono un *data breach*. Nell'agosto 2019, l'*International Organization for Standardization* (ISO) e la *International Electrotechnical Commission* (IEC) hanno pubblicato un nuovo *standard* di *privacy* per aiutare le organizzazioni che raccolgono ed elaborano informazioni personali o *personally identifiable information* (PII) a rispettare le normative internazionali sulla *privacy*. Il nuovo *standard* arriva dopo che, in Europa, l'introduzione del *General Data Protection Regulation* ha prodotto un duplice effetto, rappresentando un'innovazione e un'armonizzazione rispetto alle normative esistenti sulla *privacy* dei dati che riflettono le realtà del mondo digitale in cui viviamo attualmente[297]. Al di fuori dell'Europa, paesi

[297] ISO/IEC 27701:2019 *Security techniques — Extension to* ISO/IEC 27001 *and* ISO/IEC 27002 *for privacy information management — Requirements and guidelines*. Disponibile *online* all'indirizzo *web*: https://www.iso.org/standard/71670.html. Data di ultimo accesso e consultazione: 15 novembre 2020. Questo documento specifica i requisiti e fornisce una guida per stabilire, implementare, mantenere e migliorare continuamente un sistema di gestione delle informazioni sulla *privacy* (PIMS) sotto forma di estensione a ISO / IEC 27001 e ISO /

come Brasile, Australia, Corea e Cina, stanno creando una legislazione sulla protezione dei dati, ispirandosi, in alcuni casi, proprio ai principi espressi nel GDPR. Lo *standard* ISO/IEC 27701 di recente pubblicazione rappresenta un importante passo in avanti nella definizione di schemi di certificazione dei trattamenti di dati personali. Proprio per questo motivo, a livello internazionale (non solo in Europa) ISO ed IEC hanno deciso di predisporre uno strumento pratico sulla scia di quanto già definito in passato. Da sottolineare che queste organizzazioni avevano già intrapreso un percorso di avvicinamento alla protezione dei dati pubblicando una serie di aggiornamenti alle normative già esistenti (ad esempio: ISO/IEC 27001:2017 adottata anche in Italia dalla UNI, Ente italiano di Normazione). ISO (acronimo di *International Organization for Standardization*) è la più grande organizzazione mondiale per lo sviluppo degli *standard* normativi. A partire dal 1947 l'ISO ha pubblicato più di 20.000 standard legati a vari settori produttivi (quali agricoltura, costruzioni, ingegneria, apparati medici, *information technology*, ecc.). L'IEC (*International Electronical Commission*) è la principale organizzazione mondiale che predispone e pubblica *standard* internazionali per tutte le categorie

IEC 27002 per la gestione della *privacy* nel contesto dell'organizzazione. Questo documento specifica i requisiti relativi ai PIMS e fornisce indicazioni per i titolari e responsabili di PII che hanno la responsabilità per l'elaborazione PII. Questo documento è applicabile a tutti i tipi e le dimensioni di organizzazioni, comprese aziende pubbliche e private, enti governativi e organizzazioni *no-profit*, che sono controllori PII e / o processori PII che elaborano PII all'interno di un ISMS. Informazioni generali. *Status*: pubblicato; data di pubblicazione: agosto 2019; edizione: 1; numero di pagine: 66; comitato tecnico: ISO/IEC JTC 1/SC 27 *Information security, cybersecurity and privacy protection*; ICS: 35.030 IT *Security*.

legate ad elettrotecnica ed elettronica[298]. IEC collabora con la ISO nella predisposizione degli *standard* anche nel settore della *privacy*[299]. Il più recente di essi è stato predisposto ad agosto 2019 quando ISO ed IEC hanno pubblicato un nuovo *standard* internazionale, specificando come le organizzazioni dovrebbero gestire le informazioni

[298] Il principale organo di standardizzazione e regolamentazione è l'ISO (*International Organization for Standardization*) che è il più autorevole organismo a livello mondiale per la determinazione di regole tecniche per la valutazione e la standardizzazione dei processi in ambienti produttivi. L'ISO nasce nella sfera comunitaria come sistema di attestazione di conformità su base volontaria e competitiva della peculiarità e qualità dei processi e dei prodotti. La certificazione ISO è coordinata dall'Organizzazione Internazionale per la Standardizzazione delle procedure che disciplinano quasi tutte le attività umane. Nell'ISO confluiscono gli Enti di normativa di 157 Paesi industrializzati e in via di sviluppo di tutto il mondo. Per l'Italia le norme ISO a livello mondiale e CEN (Comitato Europeo di normazione) a livello Europeo vengono rappresentate dal consorzio privato senza scopo di lucro UNI (Ente Nazionale Italiano di Unificazione) che si occupa dell'attività normativa nei settori industriali, commerciali e nel terziario. In particolare, i compiti dell'UNI sono, tra altri, di elaborare nuove disposizioni in collaborazione con tutte le parti interessate, divulgare le norme tecniche e sostenere l'equilibrio delle norme. L'ISO collabora intrinsecamente con l'IEC (Commissione Elettrotecnica Internazionale) organizzazione internazionale responsabile della descrizione di standard in materia di elettricità, elettronica e tecnologie collegate.

[299] Le normative di interesse ai fini della valutazione del rischio *privacy* sono: UNI/ISO 31000:2018 – *Risk management — Guidelines*; ISO/IEC 29134:2017 – *Information technology — Security techniques — Guidelines for privacy impact assessment*; UNI CEI EN ISO/IEC 27001:2017 – *Information technology – Security techniques – Information security management systems – Requirements*; UNI CEI EN ISO/IEC 27002:2017 – *Information technology – Security techniques – Code of practice for information security controls*; ISO/IEC 29151:2017 – *Information technology — Security techniques — Code of practice for personally identifiable information protection*.

personali e aiutare a dimostrare la conformità rispetto alle normative vigenti sulla *privacy* (ISO/IEC 27701 e GDPR).

### 3. Il livello di accountability: responsabilità e fiducia nel trattamento delle informazioni personali

La pubblicazione e l'entrata in vigore del GDPR ha di fatto regolamentato in Europa il trattamento delle informazioni personali[300]. Ha rappresentato un salto di qualità nella regolamentazione del settore *privacy*, dal momento che ha introdotto l'importantissimo principio di *accountability*, responsabilizzando gli attori coinvolti nel trattamento dei dati personali, siano essi titolari (cioè soggetti che definiscono modalità e finalità del trattamento) o responsabili (colore che eseguono il trattamento) come definiti nell'art. 4 del GDPR. Allo stesso tempo, è stato stressato il concetto di sicurezza delle informazioni e sono stati forniti strumenti agli interessati per poter riprendere il

[300] La gestione delle informazioni sulla *privacy* è influenzata dal trattamento dei dati personali. Cfr. art. 5, par. 1 del GDPR "Principi applicabili al trattamento di dati personali". Questo trattamento è suddiviso dal GDPR in sei principi di protezione dei dati: 1. Liceità, correttezza e trasparenza: il trattamento deve essere corretto e lecito e per finalità specifiche; 2. Limitazione della finalità: il trattamento non deve essere utilizzato per nessun altro scopo; 3. Minimizzazione dei dati: le informazioni personali devono essere adeguate e pertinenti per gli scopi specificati e devono essere limitate a quanto necessario; 4. Esattezza: le informazioni personali devono essere accurate e, ove necessario, aggiornate; 5. Limitazione della conservazione: le informazioni personali non devono essere conservate più a lungo del necessario; 6. Integrità e riservatezza: le informazioni personali devono essere trattate in modo sicuro. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione») come stabilito dall'art. 5, par. 2 del GDPR.

controllo dei propri dati, o quantomeno, limitare gli impatti che da essi possono derivare. Tuttavia, il GDPR non dà istruzioni operative pragmatiche su alcuni aspetti che sono lasciati alla libera interpretazione delle singole organizzazioni. Ad esempio, presenta concetti come valutazione del rischio, certificazione dei trattamenti, ma non fornisce gli strumenti pratici che consentano alle organizzazioni di avere delle linee guida entro le quali muoversi in funzione della specificità organizzativa e del proprio settore di *business*. Molte organizzazioni hanno implementato un ISMS (*Information Security Management System*) rispettando i requisiti ed i controlli riportati nella normativa ISO/IEC 27001 la cui ultima versione è stata rilasciata nel 2017. La nuova ISO/IEC 27701 nasce proprio con l'obiettivo di implementare un PIMS (*Privacy Information Management System*) cioè un sistema per la protezione dei dati personali; quindi, un ISMS specializzato sulle tematiche peculiari della *privacy* e si pone come punto unico di riferimento in questo ambito, dal momento che referenzia gli altri *standard* vigenti in materia dei quali estende ed attualizza le indicazioni. La normativa specifica nella parte introduttiva quanto segue:

*"una organizzazione che si conformi ai requisiti del documento produrrà una serie di evidenze formali che documentano come essa gestisce i dati personali. Queste evidenze possono facilitare gli accordi con i business partner laddove la gestione dei dati personali sia un aspetto rilevante per entrambi. Queste evidenze possono anche essere di ausilio nella relazione con altri stakeholder".*

Da quanto appena esposto, è facile derivare i benefici che la ISO/IEC 27701 può avere a livello di *accountability*. Come noto, tale concetto, viene richiamato espressamente

dal GDPR ed utilizzato in particolare nella versione inglese. Nella versione italiana, si parla in modo più generale di "responsabilizzazione": in particolare al Capo II, articolo 5, paragrafo 2, dove, con riferimento al titolare del trattamento si legge "Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)". Lo stesso concetto viene anche espresso nel *considerando* n. 85. In sintesi, l'*accountability* è una responsabilizzazione diretta di chi definisce le finalità ed i mezzi (titolare) oppure esegue un trattamento di dati personali (responsabile) ed obbliga a documentare i razionali alla base di qualsiasi scelta di natura tecnica/organizzativa che riguarda l'implementazione di un trattamento. È immediata la correlazione con quanto afferma la norma: uniformandosi ai requisiti ed ai controlli della ISO/IEC 27701, tutte le scelte vengono documentate ed hanno le fondamenta in una normativa, quindi in una *best practice*, riconosciuta a livello internazionale alla quale è associato uno schema di certificazione.

## 4. Lo standard internazionale per la gestione delle informazioni sulla privacy ISO 27701: lo strumento pratico per la compliance al GDPR

È strutturato allo stesso modo della ISO / IEC 27001, quindi dall'istituzione del sistema di gestione delle informazioni sulla *privacy* (PIMS) fino alla sua revisione e adattamento[301]. Ci sono anche sezioni sulla valutazione e il

[301] Cfr. il dettagliato manuale di SHIPMAN A., WATKINS S. (2020), *ISO/IEC 27701:2019: An introduction to privacy information management*, Ely, Cambridgeshire, United Kingdom: IT Governance Publishing. Il volume è inteso per coloro che cercano informazioni generali sulla gestione delle informazioni sulla *privacy*; organizzazioni

miglioramento delle prestazioni. Tuttavia, affrontare i requisiti in quest'ordine non è un requisito in sé. Una delle sfide dello *standard* internazionale è la variazione della definizione di elaborazione delle informazioni sulla *privacy* in tutto il mondo. In effetti, la definizione di informazioni personali differisce a livello internazionale. Il comitato ISO / IEC che sviluppa *standard* relativi alla privacy (ISO / IEC JTC1 / SC27 / WG5) ha deciso il termine "informazioni di identificazione personale" (vedere ISO / IEC 29100 per una definizione) - ISO / IEC 27701 utilizza questo termine. Il GDPR dell'UE utilizza il termine "dati personali". Per risolvere questo problema, ISO / IEC 27701 consente agli utenti di adottare definizioni locali per le proprie implementazioni.

### *4.1 Definizione e contestualizzazione*

ISO / IEC 27701: 2019 è un'estensione della *privacy* allo *standard* internazionale di gestione della sicurezza delle

---

che implementano, o stanno valutando di migliorare un PIMS, in particolare laddove si sta prendendo in considerazione l'uso di ISO / IEC 27701: 2019. Consente inoltre di comprendere le basi della gestione delle informazioni sulla *privacy*, tra cui: gestione delle informazioni sulla *privacy*; come gestire con successo le informazioni sulla *privacy* utilizzando un PIMS allineato a ISO / IEC 27701; principali aree di investimento per un PIMS focalizzato sul *business*; come l'organizzazione può dimostrare il grado di sicurezza che offre in merito alla gestione delle informazioni sulla *privacy*. Questa guida si rivela utile durante una serie di fasi di qualsiasi progetto di trattamento dei dati personali. Cfr. inoltre IT GOVERNANCE (2019), *Green paper – ISO 27701 Privacy information management systems*, IT Governance Publishing. IT Governance scrive e pubblica ampiamente su GDPR, *data privacy* e *cyber security* e ha sviluppato una gamma di strumenti per la IT *governance*, *information security* e professionisti della conformità normativa.

informazioni ISO / IEC 27001 (Tecniche di sicurezza ISO / IEC 27701 - Estensione a ISO / IEC 27001 e ISO / IEC 27002 per la gestione delle informazioni sulla *privacy* - Requisiti e linee guida). La ISO 27701 specifica i requisiti e fornisce una guida per stabilire, implementare, mantenere e migliorare continuamente il *Privacy Information Management System* (PIMS), dunque un sistema di gestione delle informazioni sulla *privacy*. Questo *standard* di sicurezza delle informazioni fornisce una guida per le organizzazioni che desiderano implementare sistemi per supportare la conformità al GDPR e ad altri requisiti sulla *privacy* dei dati. Si basa sui requisiti della norma ISO/IEC 27001, lo *standard* per i sistemi di gestione della sicurezza delle informazioni (ISMS), e sul Codice di buone pratiche per i controlli della sicurezza delle informazioni nella ISO/IEC 27002. ISO 27701 prende alcune delle sue definizioni chiave da ISO 29100[302], che utilizza termini che differiscono da altre fonti[303].

---

[302] ISO/IEC 29100:2011 *Information technology — Security techniques — Privacy framework*. Lo *standard* è stato revisionato e confermato nel 2017. ISO / IEC 29100:2011 fornisce un quadro sulla *privacy* che specifica una terminologia comune; definisce gli attori e il loro ruolo nel trattamento delle informazioni di identificazione personale (PII); descrive considerazioni sulla tutela della *privacy*; e fornisce riferimenti a principi di *privacy* noti per la tecnologia dell'informazione. ISO / IEC 29100: 2011 è applicabile alle persone fisiche e alle organizzazioni coinvolte nella specifica, acquisizione, architettura, progettazione, sviluppo, *test*, manutenzione, amministrazione e gestione di sistemi o servizi di tecnologia dell'informazione e della comunicazione in cui sono richiesti controlli della *privacy* per l'elaborazione delle PII. Cfr. questo *standard* al seguente indirizzo *web*: https://www.iso.org/standard/45123.html.

[303] Informazioni di identificazione personale, *Personally identifiable information* (PII): "dati personali" nel GDPR. ISO 29100 definisce questo come "informazioni che (a) possono essere utilizzate per identificare l'interessato a cui tali informazioni si riferiscono, o (b) sono o potrebbero essere collegate direttamente o indirettamente a un

### *4.2 Integrazione sinergica ISO 27001 – ISO 27701*

ISO 27001 stabilisce i requisiti per un ISMS (sistema di gestione della sicurezza delle informazioni), un approccio basato sul rischio che comprende persone, processi e tecnologia[304]. La certificazione accreditata ISO 27001 fornisce agli *stakeholders* la garanzia che i dati siano adeguatamente protetti. Le organizzazioni che hanno implementato la ISO 27001 saranno in grado di utilizzare la ISO 27701 per estendere i loro sforzi di sicurezza per coprire la gestione della *privacy*, incluso il trattamento dei dati personali / PII (informazioni di identificazione personale), che può aiutarle a dimostrare che sono state adottate misure ragionevoli per conformarsi con le normative sulla protezione dei dati come il GDPR. Le organizzazioni senza un ISMS possono implementare ISO 27001 e ISO 27701 insieme come un unico progetto di implementazione.

---

interessato" (clausola 2.9). PII *principal*: "interessato" nel GDPR. ISO 29100 definisce questo come una "persona fisica a cui si riferiscono le informazioni di identificazione personale (PII)" (clausola 2.11). PII *controller*: "titolare del trattamento dei dati" nel GDPR. ISO 29100 lo definisce come "*privacy stakeholder* (o s*takeholder* della *privacy*) che ne determina gli scopi e i mezzi elaborazione di informazioni di identificazione personale (PII) diverse dalle persone fisiche che utilizzare i dati per scopi personali" (clausola 2.10). PII *processor*: "responsabile del trattamento dei dati" nel GDPR. ISO 29100 lo definisce come "*privacy stakeholder* che elabora le informazioni di identificazione personale (PII) per conto di e in conformità con le istruzioni di un PII *controller*" (clausola 2.12).

[304] WATKINS S. G. (2013), *An Introduction to Information Security and ISO 27001:2013. A Pocket Guide*, Second Edition, IT Governance Publishing.

### *4.3 Organizzazioni che potrebbero implementare la ISO 27701*

ISO 27701 è stata progettata per essere utilizzata da tutti i titolari del trattamento e gli incaricati del trattamento. Come la ISO 27001, ISO 27701 sostiene un approccio basato sul rischio in modo che ogni organizzazione conforme affronti i rischi specifici, nonché i rischi per i dati personali. La ISO/IEC 27701 fornisce indicazioni a qualsiasi organizzazione responsabile del trattamento delle informazioni di identificazione personale (PII) nell'ambito di un sistema di gestione della sicurezza delle informazioni. Possono beneficiarne le organizzazioni di tutte le dimensioni e tipologie, comprese le imprese pubbliche e private, nonché gli enti governativi e altri tipi di organizzazione. Fornisce un approccio basato sul rischio, aiuta le organizzazioni a prevenire rischi specifici per la *privacy* già affrontati così come i nuovi rischi per i dati personali e la *privacy*. Indipendentemente dalle dimensioni dell'organizzazione e che si tratti di un titolare o di un responsabile, è consigliabile conseguire la certificazione per la propria organizzazione o richiederla ai fornitori in base ai requisiti aziendali. Questo vale soprattutto per i responsabili, i responsabili secondari e i co-titolari che elaborano dati sensibili o elevati volumi di dati personali. In ogni caso, l'organizzazione deve valutare le proprie esigenze aziendali per determinare se le certificazioni per i propri prodotti e servizi sono idonee. Inoltre, ISO/IEC 27701:2019 è applicabile a tutti i tipi e dimensioni di organizzazioni, comprese Amministrazioni pubbliche, Enti Governativi e Organizzazioni senza scopo di lucro.

### *4.4 Differenza tra il sistema di gestione dati ISO 27701 e il servizio di gestione BS 10012*

Mentre ISO 27701 stabilisce i requisiti per un *Privacy Information Management System*, BS 10012:2017 "*Data protection – Specification for a personal information management system*" è uno degli *standard* di riferimento per la gestione delle informazioni personali[305]. C'è poca differenza sostanziale tra i due termini – entrambi sono sistemi di gestione progettati per proteggere le informazioni personali – ed è possibile utilizzare l'acronimo PIMS per fare riferimento a entrambi.

### *4.5 Altre mappature di controllo ISO 27701*

Oltre a fornire requisiti specifici per la *privacy*, controlli e obiettivi di controllo per titolari e incaricati del trattamento, ISO 27701 include allegati che li mappano a: (1) ISO 29100 (*Information technology – Security techniques – Privacy framework*); (2) ISO 29151 (*Information technology – Security techniques – Code of practice for personally identifiable information protection*); e (3) ISO 27018 (*Information technology – Security techniques – Code of practice for protection of personally identifiable*

[305] BS 10012, elaborato dalla *British Standards Institution*, è uno *standard* di sistema di gestione efficace, soprattutto per organizzazioni nel Regno Unito, poiché tiene conto non solo del GDPR ma anche del *Data Protection Act* del Regno Unito e indicazioni dello *Information Commissioner's Office*. La norma ha una struttura che si basa sul modello HLS – *High Level Structure*; in tal modo viene favorita l'integrazione tra gli altri sistemi di gestione all'interno dell'organizzazione. Cfr. *online* lo *standard* normativo al seguente indirizzo *web*: https://sistemadigestioneprivacy.it/index.php/servizi-bs-100122017/. Data di ultima consultazione: 12 novembre 2020.

*information (PII) in public clouds acting as PII processors*). Contiene anche un allegato che mappa i suoi requisiti e controlli con i requisiti del GDPR; quindi, ISO 27701 può essere utilizzato come guida alla conformità al GDPR da titolari del trattamento e responsabili del trattamento dei dati. Ad esempio, gli obblighi dei titolari del trattamento dei dati per il rispetto dei diritti degli interessati ai sensi del GDPR sono coperti dai controlli ISO 27701 che coprono gli obblighi verso gli interessati. Viene fornita una guida per l'implementazione di ciascun controllo.

### *4.6 Dimostrare la conformità al GDPR con ISO 27701 e ISO 27001*

L'implementazione di ISO 27701 e ISO 27001 consentirà di soddisfare i requisiti di *privacy* e sicurezza delle informazioni del GDPR e di altri regimi di protezione dei dati e dimostrare di disporre di accordi di gestione per "misure tecniche e organizzative appropriate" per proteggere i dati personali elaborati e difendere i diritti degli interessati, in linea con il principio di *accountability* del Regolamento (articolo 5, paragrafo 2). L'articolo 42 del GDPR discute i meccanismi di certificazione della protezione dei dati e i sigilli e i marchi di protezione dei dati. Non esistono ancora tali meccanismi. Tuttavia, è possibile ottenere una certificazione accreditata in modo indipendente secondo ISO 27001 - e per estensione ISO 27701 se si implementano i suoi controlli - che dimostrerà agli *stakeholder* e alle autorità di regolamentazione che la propria organizzazione sta seguendo le migliori pratiche internazionali quando si tratta di proteggere i dati personali.

### *4.7 Note conclusive in merito alla ISO 27001:2013*

Un sistema di gestione della sicurezza delle informazioni completo (ISMS)[306] allineato a ISO / IEC 27001:2013 potrebbe già affrontare le sfide della *data protection* e soddisfare dunque i requisiti, ma talvolta senza affrontare completamente la normativa sulla *privacy*. Ciò significa che i certificati di conformità alla ISO 27001 vengono rilasciati senza la garanzia che la protezione dei dati e le esigenze sono state adeguatamente soddisfatte. Mentre la protezione dei dati richiede naturalmente un grado di sicurezza delle informazioni (il GDPR li definisce "misure tecniche e organizzative"), l'organizzazione deve andare oltre e proteggere anche i diritti degli interessati, che non possono essere garantiti dalla sola sicurezza delle informazioni. Ottenere un certificato di conformità ISO 27701:2019 come estensione alla ISO 27001:2013 significa che le organizzazioni hanno implementato un sistema di gestione dei dati che assicuri che tutti gli aspetti rilevanti in materia di *privacy* (ex GDPR) siano presi in considerazione. Per impostazione predefinita, un certificato di conformità dà agli s*takeholder* esterni maggiore fiducia la gestione della *privacy*.

[306] WATKINS S. G. (2013), *An Introduction to Information Security and ISO 27001:2013. A Pocket Guide*, Second Edition, IT Governance Publishing.

## 5. Realizzare il Privacy Information Management System: responsabilità e fiducia nel trattamento delle informazioni personali

ISO 27701 è stato sviluppato dal comitato tecnico ISO SC27 con *input* da 25 organismi esterni, compreso il Comitato europeo per la protezione dei dati (EDPB). Un sistema di gestione della *privacy* è diverso da un ISMS, sebbene strettamente relazionato. L'approccio alla ISO 27701 riconosce che la sicurezza delle informazioni (la conservazione della riservatezza, integrità e disponibilità delle informazioni) documentata nella ISO 27001 è un aspetto chiave di un'efficace gestione della *privacy*. ISO 27701 definisce i requisiti aggiuntivi per un ISMS per coprire la *privacy* e l'elaborazione delle informazioni di identificazione personale (PII). Questi sono supportati da controlli aggiuntivi che riguardano specificamente la protezione dei dati creando ciò che lo *standard* chiama un sistema di gestione delle informazioni sulla *privacy* (PIMS). Il nuovo *standard* fissa i requisiti di elaborazione della *privacy* su un ISMS. Questo richiede che la "sicurezza delle informazioni" (ISO 27001) venga letta invece come "sicurezza delle informazioni e *privacy*" in tutti i casi (ISO27701). Per esempio, dove ISO 27001 utilizza "prestazioni di sicurezza delle informazioni", ISO 27701 lo richiede leggerlo come "sicurezza delle informazioni e prestazioni della *privacy*". Lo *standard* prosegue aggiungendo requisiti specifici per la *privacy* ad alcune delle clausole della ISO 27001 e dei controlli nell'Allegato A, e aggiunge alcune specifiche sulla *privacy* oltre i controlli esistenti sulla sicurezza delle informazioni (e ora sulla *privacy*). Infine, offre una guida che si basa su quella disponibile nella ISO 27002 soggetta se l'organizzazione in questione è un titolare del trattamento e / o responsabile del trattamento. ISO 27701 si basa anche sul principio della

sicurezza delle informazioni indirizzando il lettore ai più estesi principi sulla *privacy* in ISO / IEC 29100. Questi coprono una più ampia serie di preoccupazioni sulla *privacy*, comprese quelle contemplate nelle normative sulla protezione dei dati a livello internazionale. Dunque, il PIMS è basato su uno dei più diffusi *standard* internazionali per la gestione della sicurezza delle informazioni: ISO/IEC 27001. Se l'organizzazione ha già familiarità con ISO/IEC 27001, risulterà logico e maggiormente efficiente integrare i nuovi controlli della *privacy* del PIMS. Di conseguenza, l'implementazione e il controllo di entrambi risulteranno meno costosi e più facili da attuare. Punti chiave di ISO/IEC 27001 e PIMS: (a) ISO/IEC 27001 è uno degli *standard* ISO più usati al mondo, con numerose aziende già certificate; (b) PIMS include un nuovo titolare e controlli specifici per titolari che consentono di colmare il divario tra *privacy* e sicurezza, fornendo un punto di integrazione tra due funzioni distinte nelle organizzazioni; (c) la *privacy* dipende dalla sicurezza. Analogamente, PIMS dipende da ISO/IEC 27001 per la gestione della sicurezza. La certificazione per PIMS non può essere conseguita in modo indipendente: deve essere ottenuta come estensione di una certificazione ISO/IEC 27001. Richiedere ai fornitori la certificazione secondo lo *standard* PIMS consentirà di stabilire in modo efficace le procedure relative alla *privacy* di *partner* e fornitori, indipendentemente dalle dimensioni dell'organizzazione. ISO/IEC 27701 fornisce la soluzione a tre obblighi di conformità chiave: (1) l'eccessivo numero di requisiti normativi da gestire: soddisfare più requisiti normativi tramite l'uso di un *set* di controlli operativi che consente un'implementazione coerente ed efficiente; (2) il costo eccessivo per il controllo di ogni singola normativa: i revisori, sia interni che di terze parti, possono valutare la conformità alle normative con un controllo operativo

universale impostato in un unico ciclo di controllo; (3) i potenziali rischi del prendere accordi relativi alla conformità senza alcuna prova: gli accordi commerciali che comportano il trasferimento di informazioni personali possono garantire la certificazione di conformità[307].

### *5.1 La struttura normativa della ISO 27701 in relazione con le ISO 27001 e 27002*

La normativa è strutturata con una parte introduttiva nella quale si ribadiscono obiettivi e campo di applicazione, le altre normative di riferimento, la terminologia. Viene inoltre dettagliata la correlazione con la ISO/IEC 27001 ed ISO/IEC 27002 nella versione 2013, ciò perché la ISO/IEC 27701 di fatto costituisce un'estensione delle normative appena citate e deve essere applicata in modo congiunto ad

[307] Cfr. la guida pratica di TOIATI M. (2019), *ISO 27701 per la protezione dei dati personali: realizzare un Privacy Information Management System*, sul portale "Cyber Security 360". L'articolo è disponibile *online* al seguente indirizzo *web*: https://www.cybersecurity360.it/legal/privacy-dati-personali/iso-27701-per-la-protezione-dei-dati-personali-realizzare-un-privacy-information-management-system/. Data di ultimo accesso e consultazione: 10 novembre 2020. La guida mostra come progettare e realizzare soluzioni tecnico/organizzative conformi al GDPR e alla normativa vigente in materia di *privacy*. Cfr. inoltre BRITISH STANDARDS INSTITUTION (2019), *ISO/IEC 27701 Privacy Information Management Your implementation guide*. BSI è la società di miglioramento del *business* che consente alle organizzazioni di trasformare gli *standard* della migliore pratica in abitudini di eccellenza. Lavorando con oltre 86.000 clienti in 193 paesi, è un vero *business* internazionale con competenze ed esperienza in diversi settori, tra cui automobilistico, aerospaziale, ambiente costruito, cibo e sanità. Grazie alla sua esperienza nello sviluppo di *standard* e soluzioni di conoscenza, garanzia e servizi professionali, BSI migliora le prestazioni aziendali per aiutare i clienti a crescere in modo sostenibile, gestire il rischio e, in ultima analisi, essere più resiliente.

esse. Da notare che nella sezione 3 "*Terms, definitions and abbreviations*" si fa esplicito riferimento alle definizioni di titolare del trattamento (in inglese *controller*) e di *Privacy Information Management System*, proprio a sottolineare la focalizzazione del documento sul tema *privacy* e protezione dei dati personali. Proprio come altri *standard* ISO, ISO 27701 divide il suo contenuto per clausola[308]. Le clausole 5–8 stabiliscono i requisiti aggiuntivi e le modifiche da applicare a ISO 27001 e meritano particolare attenzione[309].

[308] Si riportano in nota le Clausole 1 – 4 che meritano minore attenzione rispetto alle Clausole 5 – 8. Clausola 1: ambito. Questa clausola stabilisce i requisiti per la gestione del sistema e la sua applicazione prevista. ISO / IEC 27701 ha lo scopo di fornire i requisiti e una guida per stabilire, implementare, mantenere e migliorare un sistema di gestione delle informazioni sulla *privacy* sotto forma di estensione alla ISO / IEC 27001 e ISO / IEC 27002. Incentrato sui PII *controller* e PII *processor* che detengono la responsabilità per l'elaborazione delle informazioni personali. Clausola 2: riferimenti normativi. I riferimenti normativi sono documenti a cui si fa riferimento in tutto lo *standard*. Per ISO / IEC 27701 si include: ISO/IEC 27000 *Information security management systems – overview and vocabulary*, ISO/IEC 27001 *Information security management systems – requirements*, ISO/IEC 27002 *Code of practice for information security controls*, ISO/IEC 29100 *Privacy framework*. Clausola 3: termini e definizioni. Questa sezione fornisce un paio di definizioni aggiuntive per i termini importanti utilizzati in tutto lo *standard* che non sono inclusi in ISO / IEC 27000 e ISO / IEC 29100. Clausola 4: generale. Questa clausola definisce la scena per ISO / IEC 27701 e fornisce una panoramica della struttura dei documenti e indica, ad alto livello, l'ubicazione del PIMS requisiti specifici in relazione alla ISO / IEC 27001 e ISO / IEC 27002.

[309] La clausola rappresenta un requisito che deve essere rispettato ed implementato da un'organizzazione per essere *compliance* alla ISO/IEC 27701. In realtà la normativa ISO/IEC 27701:2019 utilizza il termine *should*.

Clausola nr. 5: requisiti specifici del PIMS

Questa sezione affronta ogni clausola della ISO 27001 e identifica dove il contenuto aggiuntivo è necessario. La maggior parte delle clausole ISO 27001 rimangono invariate, con l'avvertenza che la ISO 27701 richiede all'organizzazione di riconoscere la necessità della protezione dei dati nel contesto. Un'altra importante aggiunta che dovrà essere presa in considerazione riguarda la valutazione del rischio, che dovrà tenere conto del ruolo dell'organizzazione in relazione alle PII, ovvero se si tratta di un *controller* o un *processor* e come ciò potrebbe influire sui rischi per le PII. Un'altra voce riconosce l'esistenza dei nuovi *set* di controllo e consente all'organizzazione di riconciliare i propri controlli rispetto a una gamma più ampia di controlli, inclusi quelli della ISO 27701[310].

Clausola nr. 6: normativa specifica per il PIMS

Questa sezione fornisce contenuti aggiuntivi per la normativa in merito al controllo stabilita nella ISO 27002. Stabilisce un emendamento di primo livello che fa riferimento alla *information security* che dovrebbe essere considerata comprendente la protezione della *privacy*. I controlli con un impatto potenzialmente significativo sulla

[310] La clausola 5 riprende nel dettaglio tutte le clausole già definite anche nella ISO/IEC 27001 e le dettaglia in modo da considerare gli aspetti peculiari dei dati personali. È in questa sezione che vengono ripresi, ad esempio, i concetti di *risk management* e vengono ripercorse le fasi di identificazione, valutazione e trattamento del rischio. Sempre nell'ambito di questa clausola vengono rappresentati tutti gli aspetti legati alla comprensione del contesto organizzativo/operativo, alla *leadership*, al supporto, alle competenze, all'*operation*, al *performance management*.

*privacy* e sulla protezione dei dati sono coperti da un'ampia guida *extra* all'implementazione più dettagliata sulla gestione degli incidenti, supporti rimovibili, accesso degli utenti ai sistemi e servizi che elaborano PII, protezione crittografica, riassegnazione dello spazio di archiviazione che in precedenza memorizzavano PII, *backup* e ripristino di PII, recensioni del registro eventi, politiche di trasferimento delle informazioni e accordi di riservatezza[311].

Clausola nr. 7: indicazioni aggiuntive per i titolari del trattamento dati

Questa clausola fornisce una normativa sui controlli dell'allegato A della ISO 27701, che sono specifici alla *privacy* per gli scopi dei titolari delle PII. Questi controlli affrontano molti delle aree critiche della protezione dei dati e della *privacy* che non sono prese in considerazione dai controlli previsti dalla ISO 27001[312].

[311] La clausola 6 riprende nel dettaglio le linee guida espresse nella ISO/IEC 27002 specializzandole all'ambito *privacy* e protezione dati personali. Si tratta quindi di indicazioni relative all'implementazione delle misure di mitigazione del rischio (ovviamente in questo caso si tratta di rischio *privacy*). Viene fornita una guida più chiara sui ruoli e responsabilità in relazione al trattamento dei dati. Questo include la consapevolezza della segnalazione degli incidenti e le conseguenze di una violazione della *privacy*.

[312] La clausola 7 esprime condizioni addizionali specifiche per i titolari del trattamento. Vengono in particolare presi in considerazione requisiti di legge ed affrontati aspetti come la raccolta del consenso da parte dell'interessato al trattamento, il tema del legittimo interesse, la PIA (*Privacy Impact Assessment*), il rapporto con i responsabili del trattamento, la contitolarità, il registro dei trattamenti, le informative, l'esercizio dei diritti, la *privacy by default* e *by design*, la *data retention* (limitazione della conservazione dei dati), il trasferimento dati. Risulta

Clausola nr. 8: indicazioni aggiuntive per i responsabili del trattamento dati

Questa clausola fornisce una normativa sui controlli dell'allegato B della ISO 27701, che sono specifici alla *privacy* per gli scopi dei responsabili delle PII. Questi controlli affrontano molte delle aree critiche della protezione dei dati e della *privacy* che non sono prese in considerazione dai controlli previsti dalla ISO 27001[313].

Sono inoltre presenti sei allegati[314] (in inglese *Annex*) che riportano sia controlli (cioè misure tecnico/organizzative di mitigazione del rischio *privacy*)[315], sia riferimenti alle altre normative ISO/IEC vigenti.

---

evidente che questa clausola riguarda tutte le tematiche principali per la protezione dei dati personali. I requisiti vengono espressi in modo generale e poi contestualizzati ad un ambito normativo specifico, qual è il GDPR, nell'*Annex* D.

[313] La clausola 8 è dunque analoga alla 7 ma focalizzata sui responsabili del trattamento. La norma è delineata per identificare e mantenere i documenti necessari per aiutare a dimostrare la conformità con l'elaborazione delle PII concordate. Si tratta di una guida dettagliata per aiutare a rispondere alle singole richieste dei clienti, gestendo *file* temporanei creati durante l'elaborazione, la restituzione, il trasferimento o smaltimento delle informazioni personali in modo sicuro. Infine, la guida alla condivisione, al trasferimento e alla divulgazione dei dati è dettagliata per affrontare i trasferimenti giurisdizionali, i requisiti di terze parti e del subappaltatore e gestione di divulgazioni PII legalmente vincolanti.

[314] Gli allegati A e B riguardano rispettivamente titolari e responsabili del trattamento, mentre gli allegati C - F forniscono conoscenze aggiuntive che possono supportare la creazione e il funzionamento di un PIMS efficace.

[315] Il termine "controllo" indica una misura di mitigazione del rischio e che, in questo caso, si considera il rischio *privacy* derivante dalla gestione della sicurezza dei dati personali. La ISO/IEC 27701

Nel dettaglio:

Allegato A: un elenco di controlli per i titolari del trattamento dati

Analogamente alla ISO/IEC 27001 questo allegato riporta i controlli che devono essere implementati in un PIMS da un'organizzazione che si configuri come titolare del trattamento (indipendentemente dal fatto che impieghi un responsabile del trattamento o che si configuri anche come contitolare)[316].

Allegato B: un elenco di controlli per i responsabili del trattamento dati

Riporta i controlli che devono essere implementati in un PIMS da un'organizzazione che si configuri come responsabile del trattamento (indipendentemente dal fatto che si avvalga di sub-responsabili)[317].

---

fornisce un elenco di controlli obbligatori che estendono e specializzano quelli indicati nella ISO/IEC 27001. Sono previsti 31 controlli per l'Allegato A e 18 controlli per l'Allegato B, entrambi divisi in 4 identiche categorie: 1. *Conditions for collection and processing*; 2. *Obligations to PII principles*; 3. *Privacy by design and by default*; 4. *PII sharing, transfer and disclosure*.

[316] L'allegato A è focalizzato sui titolari del trattamento. I controlli riguardano in particolare: condizioni per l'acquisizione ed il trattamento dei dati; obblighi nei confronti degli interessati al trattamento; *privacy by design* e *privacy by default*; condivisione e trasferimento dei dati.

[317] I controlli dell'allegato B riguardano i responsabili del trattamento e sono focalizzati sulle stesse tematiche. Per ciascun controllo viene fornito l'ambito e l'obiettivo.

Allegato C: mappatura dei controlli per i titolari del trattamento dati sui principi sulla *privacy* ISO / IEC 2900

Riporta la mappatura rispetto alla normativa ISO/IEC 29100 *Information Technology – Privacy Techniques – Privacy Framework*[318].

Allegato D: mappatura delle clausole ISO / IEC 27701 agli artt. 5 – 49 GDPR, escluso art. 43

Allegato che riporta il *mapping* delle clausole ISO/IEC 27701 rispetto agli adempimenti ed ai concetti chiave del GDPR[319].

Allegato E: mappatura delle clausole ISO / IEC 27701 a ISO/IEC 27018 e ISO/IEC 29151

Contiene la mappatura rispetto alle normative ISO/IEC 27018 *Information Technology – Security Techniques –*

[318] L'allegato C mostra un'indicazione di come la conformità ai requisiti e controlli della ISO / IEC 27701 si riferiscono a principi sulla *privacy* in ISO / IEC 29100.

[319] L'allegato D riporta nel dettaglio la corrispondenza tra le clausole ISO/IEC 27701 e gli articoli del GDPR (mappatura delle clausole ISO / IEC 27701 agli artt. 5 – 49 GDPR, escluso art. 43). Questo mostra come la conformità a requisiti e controlli della ISO / IEC 27701 può essere rilevante per adempiere agli obblighi del GDPR e rappresenta uno strumento potentissimo per l'implementazione del principio di *accountability* e, allo stesso tempo, uno schema per l'*audit* e la certificazione dei trattamenti secondo quanto previsto dal Regolamento. L'allegato D è strutturato a tabella che riporta nella prima colonna le clausole e sotto-clausole della ISO/IEC 27701 e nella seconda colonna l'articolo GDPR di riferimento indicando anche il paragrafo e la lettera.

*Code of Practice for Protection of Personally Identifiable Information (PII) in public clouds acting as PII* e alla ISO/IEC 29151 *Information Technology – Security Techniques – Code of Practice for Personally Identifiable Information Protection*.

Allegato F: dettagli su come applicare ISO / IEC 27701 a ISO / IEC 27001 e ISO / IEC 27002

Descrive ulteriori modalità per applicare la ISO/IEC 27001 ed ISO/IEC 27002 all'ambito *privacy* laddove vengano trattati dati personali[320].

### *5.2 Vantaggi della implementazione del PIMS*

Una volta implementato lo *standard* ISO/IEC 27701:2019, è indispensabile che l'organizzazione ne misuri l'efficacia, al fine di assicurarsi della scelta delle contromisure adottate

[320] Mappa chiaramente l'estensione dei termini di sicurezza delle informazioni per incorporare la *privacy* e include alcuni esempi per l'applicazione. Applicazione della ISO 27701:2019 – Importanza dell'Allegato F. Si dovrebbe iniziare a leggere questo *standard* leggendo prima l'ultimo allegato – cioè l'allegato F – Come applicare ISO/IEC 27701 a ISO/IEC 27001 e ISO/IEC 27002. L'allegato F fa riferimento a tre casi per l'applicazione della ISO 27701 alla protezione della *privacy* dei principali PII durante la loro elaborazione: 1. Applicazione degli *standard* di sicurezza AS-IS; 2. Aggiunte agli *standard* di sicurezza: *Privacy* aggiuntiva – requisiti specifici o guida all'implementazione; 3. Perfezionamento degli *standard* di sicurezza: gli *standard* di riferimento sono perfezionati dai requisiti specifici sulla *privacy* o dalle linee guida per l'implementazione. Cfr. KHAMESRA S. (CEO – PRICORIS LLP) (2021), *Implementing ISO 27701:2019 PIMS – Two common fallacies*, fondata nel 2019, è una indipendente società di consulenza sulla sicurezza: https://pricoris.com/implementing-iso-27701/.

per contenere il rischio al livello stabilito e come le soluzioni, anche in termini di procedure operative, potrebbero essere migliorate. Il *framework* è stato progettato in modo da essere flessibile e consentire alle organizzazioni di definire e realizzare i propri obiettivi di sicurezza in tema di *privacy*, apportando i necessari adeguamenti nel tempo. I vantaggi di certificarsi ISO/IEC 27701:2019 sono: (a) raggiungere un elevato livello di *accountability*, soprattutto nei confronti dell'autorità di controllo; (b) generare fiducia nei confronti di clienti ed interessati del trattamento circa la capacità dell'impresa di gestire correttamente i dati personali e fornire trasparenza agli *stakeholder* e facilitare dunque accordi commerciali; (c) definire i ruoli e le responsabilità all'interno dell'organizzazione e sviluppare competenze e sensibilità interna sul tema del trattamento dei dati personali; (d) comprovare la conformità al GDPR ed alle normative vigenti in materia di protezione dei dati personali, nel rispetto dei principi di *privacy by design* e *by default*; (e) ridurre la complessità integrandosi con il principale *standard* di Sicurezza delle Informazioni ISO/IEC 27001 e migliorare i processi aziendali volti a evitare infrazioni alla normativa; (f) dotarsi di un sistema per la gestione dei *data breach* e delle richieste degli interessati e dotarsi delle misure idonee a tutela dei dati trattati.

### *5.3 Requisiti legali, regolamentari e contrattuali e rischio d'impresa*

Il trattamento dei dati personali è disciplinato nella maggior parte dei Paesi da leggi e / o regolamenti. Pertanto, qualsiasi elaborazione deve essere eseguita nell'ambito delle norme locali. Inoltre, laddove l'organizzazione agisce in qualità di responsabile del trattamento dei dati, saranno

in atto requisiti contrattuali che determinano il modo in cui l'organizzazione deve agire per garantire che le regole locali non siano compromesse. Pertanto, i requisiti specifici di un sistema di gestione delle informazioni sulla *privacy* (PIMS) devono essere determinati alla luce delle regole locali e dei requisiti contrattuali appropriati. Questi requisiti dovranno essere definiti dall'organizzazione, utilizzando tutte le risorse disponibili. Ciò potrebbe includere: *top management*; responsabile della protezione dei dati (DPO) o altra competenza legale simile; personale operativo *senior*; gestione dei *record*; risorse umane; *information security*; competenza tecnica di IT; gestione del rischio; vendite e *marketing*. Sarà necessario includere il *top management* in modo che la direzione aziendale (sotto forma di politiche aziendali) possa essere concepita e concordata. La competenza legale dovrà essere aggiornata con la legislazione e le normative vigenti in tutti i Paesi coperti dall'organizzazione. In alcuni Paesi, alcune organizzazioni sono tenute a impiegare (internamente o esternamente) una persona adeguatamente qualificata per coprire questa competenza legale, indicata nel GDPR con il termine "responsabile della protezione dei dati". Il personale operativo *senior* dovrà fornire *input* sulle procedure operative utilizzate e su come queste implementano le politiche aziendali. Coloro che hanno responsabilità di gestione dei *record* avranno conoscenza di come i *record* vengono acquisiti / creati all'interno dell'organizzazione, dove sono archiviati e i periodi di conservazione appropriati. Le risorse umane dovranno essere coinvolte se il trattamento delle informazioni personali relative ai dipendenti rientra nell'ambito del PIMS. Le risorse umane capiranno quali informazioni personali detengono, come vengono gestite e per quanto tempo vengono conservate. La sicurezza delle informazioni e / o l'IT saranno a conoscenza dei sistemi

utilizzati per gestire le informazioni personali e di come sono protetti da accessi non autorizzati. La gestione del rischio comprenderà il profilo di rischio dell'organizzazione e sarà in grado di fornire consigli sulla gestione del rischio ove necessario. Il personale addetto alla gestione del rischio, insieme alle competenze legali sopra descritte, dovrebbe essere in grado di eseguire le valutazioni necessarie dell'impatto sulla *privacy* (PIA), a volte chiamate valutazione dell'impatto sulla protezione dei dati (DPIA), per determinare i necessari controlli sulla *privacy* su cui l'organizzazione farà affidamento. Le vendite e il *marketing* avranno le proprie esigenze di informazioni personali e devono essere coinvolte per garantire che i loro requisiti siano soddisfatti dal PIMS[321].

## 6. Audit e controlli

È importante, sia a breve che a lungo termine, essere in grado di dimostrare come sono state formulate le politiche aziendali, le procedure operative e le istruzioni di lavoro. È probabile che l'organizzazione ritenga utile conservare i registri degli sviluppi e delle attività su cui può fare riferimento in caso di necessità in futuro. Da qui il requisito che molti di questi elementi siano registrati e che l'organizzazione conservi registrazioni appropriate per tutto il tempo necessario. È anche importante creare registrazioni delle attività operative, ai fini della revisione e del processo decisionale. Questi *record* possono

[321] BAKER A. (2020), *ISO/IEC 27701 and the privacy information management system requirements*, IT Governance European Blog. L'articolo è disponibile *online* al seguente indirizzo *world wide web*: https://www.itgovernance.eu/blog/en/iso-iec-27701-and-the-privacy-information-management-system-requirements. Data ultimo accesso e consultazione: 13 novembre 2020.

includere dati di *audit trail*, sia in forma manuale che automatica. Questi *record* devono essere salvaguardati una volta creati, assicurando che solo le persone appropriate abbiano accesso ad essi e che possa essere dimostrata l'integrità dei loro contenuti. Le procedure operative devono descrivere i processi che supportano le politiche aziendali e spiegare chi fa cosa, dove e quando. Le istruzioni di lavoro potrebbero essere introdotte per dettagliare come vengono svolte determinate attività. Tutta la documentazione deve essere stata scritta e approvata dalle persone giuste e si deve garantire che solo le ultime versioni approvate siano disponibili per coloro che devono conoscerle e seguirle.

### *6.1 Auditing*

Gli *audit* possono essere effettuati a livello interno o esterno. L'*auditing* dei sistemi di gestione in generale (e un PIMS in particolare) ha l'obiettivo di dimostrare che il sistema di gestione è conforme ai requisiti dell'organizzazione, è conforme ai requisiti dello *standard* internazionale appropriato ed è efficacemente implementato e mantenuto[322]. Pertanto, l'obiettivo principale di un programma di *audit* del sistema di gestione è monitorare la conformità tra i requisiti del sistema di gestione e le pratiche di lavoro. Tali *audit* possono essere effettuati internamente, dalla funzione di *audit* di un'organizzazione o da persone che hanno familiarità con i programmi di *audit* e possono agire indipendentemente

[322] Non ci sono categorie specifiche nella ISO 27701 che si occupano di conformità e *audit*; tuttavia, lo *standard* internazionale è stato sviluppato per allinearsi alla ISO 27001 e alla ISO 27002, che contengono queste categorie e si occupano della dimostrazione della conformità legale e tecnica.

dall'operazione che stanno controllando, o esternamente da revisori specializzati. In genere, gli *audit* comportano la selezione dei singoli processi di lavoro e la verifica della pratica effettiva rispetto ai requisiti. I rapporti di *audit* identificheranno eventuali non conformità tra la pratica effettiva ei requisiti. L'organizzazione dovrà rivedere tutte le non conformità identificate e apportare gli opportuni aggiustamenti, alle pratiche di lavoro o, ove rientri nelle loro competenze, al requisito. Gli *audit* forniscono anche l'opportunità di miglioramento. Pertanto, i programmi di *audit* e gli obiettivi del programma di *audit* possono includere l'identificazione di potenziali miglioramenti al PIMS. Ciò potrebbe includere aggiornamenti alla politica (forse indotti da modifiche alla legislazione, ai regolamenti e alla loro interpretazione), procedure operative e/o istruzioni di lavoro. Laddove sono state identificate aree di interesse specifiche, potrebbero informare la selezione dei singoli processi di lavoro[323].

### *6.2 Controllo di gestione*

Il *top management* (l'alta direzione, definita in termini di sistema di gestione come una 'persona o gruppo di persone che dirige e controlla un'organizzazione al livello più alto' - dove l'organizzazione è quella nell'ambito del PIMS) ha un ruolo significativo nella gestione dei sistemi di gestione

[323] L'organizzazione dovrebbe essere a conoscenza e rispettare i propri obblighi legali e requisiti contrattuali. I *test* tecnici del PIMS dovrebbero riportare il grado in cui le apparecchiature IT, i sistemi, il *software* e i processi correlati sono come dovrebbero essere. Il programma può includere controlli per confermare che solo l'attrezzatura corretta e approvata sia collegata alla rete e che il sistema e il *software* siano quelli richiesti e può includere *test* di penetrazione per confermare la resilienza delle misure tecniche in atto.

come il PIMS. Avviano lo sviluppo del sistema di gestione, approvano le risorse necessarie e approvano le politiche aziendali che definiscono gli obiettivi del sistema di gestione. È quindi opportuno che il *top management* riesamini l'andamento del PIMS dal suo inizio fino al suo funzionamento, assicurandosi che sia efficace e soddisfi i requisiti aziendali, nel tempo. È opportuno effettuare riesami della direzione a intervalli regolari (ad esempio ogni 12 mesi) per raggiungere questi obiettivi. Queste revisioni potrebbero prendere in considerazione rapporti di *audit*, eventuali modifiche alla legislazione, ai regolamenti, eventuali incidenti relativi alla *privacy* e suggerimenti del personale operativo. La revisione potrebbe anche esaminare le misure di efficacia che sono state sviluppate e le opportunità di miglioramento continuo che sono state identificate o implementate[324].

## 7. Certificazione e accreditamento

La certificazione è «il rilascio da parte di un organismo indipendente di un'assicurazione scritta (un certificato) del fatto che il prodotto, il servizio o il sistema in questione soddisfa requisiti specifici»; nella norma EN-ISO/IEC 17000:2004 a cui la ISO 17065 fa riferimento, la certificazione è definita come "attestazione di terza parte (…) relativa a prodotti, processi e servizi". La certificazione in sé non è prova di conformità, ma rappresenta un elemento utilizzabile per la dimostrazione della conformità e per tali motivi è necessario attuarla con le modalità previste dal Regolamento, in termini di

[324] Cfr. l'ampio contributo di SHIPMAN A., WATKINS S. (2020), *ISO/IEC 27701:2019: An introduction to privacy information management*, Ely, Cambridgeshire, United Kingdom: IT Governance Publishing, in particolare capp. 3 e 4.

trasparenza, esperienza e metodo. L'articolo 42 del GDPR riguarda gli schemi di certificazione, affermando che gli Stati membri, le autorità di vigilanza, l'EDPB e la Commissione europea dovrebbero incoraggiare schemi che dimostrano la conformità al Regolamento[325]. La

[325] Cfr. articolo 42 GDPR *Certificazione*: 1. Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese. 2. Oltre all'adesione dei titolari del trattamento o dei responsabili del trattamento soggetti al presente regolamento, i meccanismi, i sigilli o i marchi approvati ai sensi del paragrafo 5 del presente articolo, possono essere istituiti al fine di dimostrare la previsione di garanzie appropriate da parte dei titolari del trattamento o responsabili del trattamento non soggetti al presente regolamento ai sensi dell'articolo 3, nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali alle condizioni di cui all'articolo 46, paragrafo 2, lettera f). Detti titolari del trattamento o responsabili del trattamento assumono l'impegno vincolante e azionabile, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati. 3. La certificazione è volontaria e accessibile tramite una procedura trasparente. 4. La certificazione ai sensi del presente articolo non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti a norma degli articoli 55 o 56. 5. La certificazione ai sensi del presente articolo è rilasciata dagli organismi di certificazione di cui all'articolo 43 o dall'autorità di controllo competente in base ai criteri approvati da tale autorità di controllo competente ai sensi dell'articolo 58, paragrafo 3, o dal comitato, ai sensi dell'articolo 63. Ove i criteri siano approvati dal comitato, ciò può risultare in una certificazione comune, il sigillo europeo per la protezione dei dati. 6. Il titolare del trattamento o il responsabile del trattamento che sottopone il trattamento effettuato al meccanismo di

certificazione ISO 27701 non soddisferà i requisiti del GDPR per uno schema di certificazione. Difatti, l'articolo 43 del GDPR richiede l'esecuzione di qualsiasi schema di certificazione secondo uno schema accreditato ISO 17065[326]. ISO 27701, tuttavia, cadrà sotto ISO 17021-1 e

certificazione fornisce all'organismo di certificazione di cui all'articolo 43 o, ove applicabile, all'autorità di controllo competente tutte le informazioni e l'accesso alle attività di trattamento necessarie a espletare la procedura di certificazione. 7. La certificazione è rilasciata al titolare del trattamento o responsabile del trattamento per un periodo massimo di tre anni e può essere rinnovata alle stesse condizioni purché continuino a essere soddisfatti i requisiti pertinenti. La certificazione è revocata, se del caso, dagli organismi di certificazione di cui all'articolo 43 o dall'autorità di controllo competente, a seconda dei casi, qualora non siano o non siano più soddisfatti i requisiti per la certificazione. 8. Il comitato raccoglie in un registro tutti i meccanismi di certificazione e i sigilli e i marchi di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato.

[326] Cfr. articolo 43 GDPR *Organismi di certificazione*: 1. Fatti salvi i compiti e i poteri dell'autorità di controllo competente di cui agli articoli 57 e 58, gli organismi di certificazione in possesso del livello adeguato di competenze riguardo alla protezione dei dati, rilasciano e rinnovano la certificazione, dopo averne informato l'autorità di controllo al fine di consentire alla stessa di esercitare i suoi poteri a norma dell'articolo 58, paragrafo 2, lettera h), ove necessario. Gli Stati membri garantiscono che tali organismi di certificazione siano accreditati da uno o entrambi dei seguenti organismi: a) dall'autorità di controllo competente ai sensi degli articoli 55 o 56; b) dall'organismo nazionale di accreditamento designato in virtù del regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio (20) conformemente alla norma EN-ISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo competente ai sensi degli articoli 55 o 56. 2. Gli organismi di certificazione di cui al paragrafo 1 sono accreditati in conformità di tale paragrafo solo se: a) hanno dimostrato in modo convincente all'autorità di controllo competente di essere indipendenti e competenti riguardo al contenuto della certificazione; b) si sono impegnati a rispettare i criteri di cui all'articolo 42, paragrafo 5, e approvati dall'autorità di controllo competente ai sensi degli articoli 55 o 56 o dal comitato, ai sensi dell'articolo 63; c) hanno istituito

procedure per il rilascio, il riesame periodico e il ritiro delle certificazioni, dei sigilli e dei marchi di protezione dei dati; d) hanno istituito procedure e strutture atte a gestire i reclami relativi a violazioni della certificazione o il modo in cui la certificazione è stata o è attuata dal titolare del trattamento o dal responsabile del trattamento e a rendere dette procedure e strutture trasparenti per gli interessati e il pubblico; e) hanno dimostrato in modo convincente all'autorità di controllo competente che i compiti e le funzioni da loro svolti non danno adito a conflitto di interessi. 3. L'accreditamento degli organi di certificazione di cui ai paragrafi 1 e 2 del presente articolo ha luogo in base ai criteri approvati dall'autorità di controllo competente ai sensi degli articoli 55 o 56 o dal comitato, ai sensi dell'articolo 63. In caso di accreditamento ai sensi del paragrafo 1, lettera b), del presente articolo, tali requisiti integrano quelli previsti dal regolamento (CE) n. 765/2008 nonché le norme tecniche che definiscono i metodi e le procedure degli organismi di certificazione. 4. Gli organismi di certificazione di cui al paragrafo 1 sono responsabili della corretta valutazione che comporta la certificazione o la revoca di quest'ultima, fatta salva la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento. L'accreditamento è rilasciato per un periodo massimo di cinque anni e può essere rinnovato alle stesse condizioni purché l'organismo di certificazione soddisfi i requisiti. 5. L'organismo di certificazione di cui al paragrafo 1 trasmette all'autorità di controllo competente i motivi del rilascio o della revoca della certificazione richiesta. 6. I requisiti di cui al paragrafo 3 del presente articolo e i criteri di cui all'articolo 42, paragrafo 5, sono resi pubblici dall'autorità di controllo in forma facilmente accessibile. Le autorità di controllo provvedono a trasmetterli anche al comitato. Il comitato raccoglie in un registro tutti i meccanismi di certificazione e i sigilli di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato. 7. Fatto salvo il capo VIII, l'autorità di controllo competente o l'organismo nazionale di accreditamento revoca l'accreditamento di un organismo di certificazione di cui al paragrafo 1 del presente articolo, se le condizioni per l'accreditamento non sono, o non sono più, rispettate o se le misure adottate da un organismo di certificazione violano il presente regolamento. 8. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 92 al fine di precisare i requisiti di cui tenere conto per i meccanismi di certificazione della protezione

quindi non soddisferà i requisiti del GDPR[327]. Ci sono buone probabilità che un eventuale schema ISO 17065 includa la certificazione ISO 27701, ma nel complesso sarà più robusto e quindi più costoso. Quelle organizzazioni che vogliono dimostrare un certo grado di sicurezza senza la spesa di uno schema accreditato ISO 17065 potrebbero optare per la certificazione ISO 27701 come compromesso economico. Data l'ampia accettazione della ISO 27001 come modello di *information security*, è probabile che molti mercati accetteranno la certificazione ISO 27701

---

dei dati di cui all'articolo 42, paragrafo 1. 9. La Commissione può adottare atti di esecuzione per stabilire norme tecniche riguardanti i meccanismi di certificazione e i sigilli e marchi di protezione dei dati e le modalità per promuovere e riconoscere tali meccanismi di certificazione, i sigilli e marchi di protezione dei dati. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

[327] Lo schema di certificazione considerato più vicino ai dettami del GDPR è stato identificato nella norma ISO/IEC 27701:2019 "*Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*", fino al 13 dicembre 2019 quando Accredia ha emanato la Circolare Tecnica 17/2019 statuendo che "se molti argomenti trattati dalla Norma ISO/IEC 27701:2019 hanno riscontro in specifici requisiti di legge nazionali, sia in Italia, sia in altri Paesi dell'Unione Europea, disciplinati dal GDPR e dalle precedenti leggi nazionali, la norma, basandosi sulla ISO 17021-1, non è da considerarsi valida ai fini del GDPR, che prevede invece una certificazione accreditata IS0 17065". Ne consegue che la certificazione ISO/IEC 27701 è fuori scopo, in quanto richiede l'accreditamento degli OdC per i sistemi di gestione (ISO 17021-1) e non ISO 17065 art. 43.1(b) e C. 100. A fronte di questo chiarimento ufficiale, oggi le aziende, PMI, microimprese e pubbliche amministrazioni che intendono perseguire una certificazione accreditata ISO 17065 in termini GDPR possono far riferimento solo alla norma ISDP©10003:2018 "Schema internazionale per la valutazione della conformità al Regolamento europeo 2016/679" accreditato da Accredia secondo la norma UNI EN ISO 17065 e liberamente scaricabile tramite il sito *web* dell'OdC IN-Veo.

come adeguata prova che l'organizzazione ha adottato misure appropriate per garantire la protezione dei dati. In ogni caso, le opzioni per la certificazione accreditata ISO 27701 dovranno evolversi poiché gli schemi attuali non lo soddisfano. Nel frattempo, l'opzione più vicina per la certificazione accreditata si farà riferimento alla ISO 27701 come fonte di controlli in una Dichiarazione di applicabilità (*Statement of applicability* o SOA) citata in un documento di certificazione accreditato per ISO 27001. Questo metodo è attualmente utilizzato per includere *standard* settoriali nelle certificazioni, ma questo sta cambiando: un emendamento in sospeso alla ISO 27006 (che stabilisce i requisiti di accreditamento per gli organismi di certificazione che offrono la certificazione ISO 27001) afferma che questo riferimento può riferirsi solo alla fonte dei controlli dettagliati nella SOA; non dovrebbe implicare la conformità a un insieme di sistemi di gestione requisiti. Indipendentemente dal risultato, è solo questione di tempo prima che ci sia un metodo per le organizzazioni di dimostrare la conformità con ISO 27701[328]. È probabile che diventi un approccio popolare alla gestione della protezione dei dati e della *privacy*, anche se la certificazione allo *standard* non è formalmente adottata come a meccanismo di certificazione ai sensi del GDPR[329].

---

[328] Qualunque sia la decisione dell'*European Data Protection Board* (EDPB) su questo tema, la normativa in oggetto rimane un tassello fondamentale nella progettazione e realizzazione di trattamenti di dati personali che salvaguardino libertà e diritti fondamentali degli interessati.

[329] Alla luce di questi razionali, la normativa ISO/IEC 27701 si poneva come candidato ideale per realizzare uno schema di certificazione dei trattamenti di dati personali come previsto dal GDPR al Capo IV, Sezione 5 – Codici di condotta e certificazioni, oltre che in diversi Considerando (98,99,100,167,168).

# SEZIONE TERZA

## RICERCA EMPIRICA
## E IMPLICAZIONI PER IL MANAGEMENT

# CAPITOLO 5

# RICERCA EMPIRICA

**SOMMARIO:** 1. Introduzione – 2. Protocollo metodologico – 3. Elaborazione e analisi dei dati – 4. Presentazione e discussione dei risultati – 5. Limiti della ricerca e traiettorie di ricerca futura – 6. Conclusioni e implicazioni per il management – 7. Appendice della ricerca.

## 1. Introduzione

La protezione dei dati in sé rappresenta una nuova forma di responsabilità sociale d'impresa. Nessun quadro giuridico presente o imminente sarà in grado di regolare efficacemente la società contemporanea massimizzando perfettamente i benefici per i consumatori e al contempo minimizzando efficacemente i rischi che le nuove tecnologie pongono. A seguito dell'entrata in vigore del Regolamento generale sulla protezione dei dati (GDPR), le imprese hanno cessato di considerare la protezione dei dati come semplice obbligo di conformità legale. Nello scenario che si sta configurando, sempre più incentrato sui dati, le imprese devono considerare la *privacy* come risorsa che aiuta a perseguire responsabilmente i propri obiettivi economici. Una solida politica aziendale può consentire l'elaborazione dei dati in modo sostenibile e promuovere il loro potenziale, seguendo regole socialmente responsabili di protezione, quali, a titolo meramente esemplificativo e non esaustivo: l'integrazione della protezione e della sicurezza dei dati nella progettazione dei processi, la trasparenza con i consumatori nella fase di raccolta dei dati

e il bilanciamento dei profitti con i benefici effettivi per i consumatori. La ricerca empirica che viene presentata in questo capitolo ha come riferimento l'adozione volontaria da parte delle imprese della nuova normativa ISO 27701, considerata la prima certificazione sulla *privacy* allineata con il GDPR riconosciuta a livello globale, che rappresenta l'estensione alla *privacy* dello *standard* di gestione della sicurezza delle informazioni ISO 27001, basato sugli stessi requisiti, controlli e obiettivi. Mentre normalmente la questione della *privacy* è considerata soprattutto dal punto di vista legale, questa nuova certificazione non solo fornisce un mezzo per dimostrare facilmente la *compliance*, ma anche un quadro strutturato su come affrontarla al meglio, raccomandando la sicurezza delle informazioni e i requisiti di protezione dei dati personali e delineando una guida pratica per la gestione di programmi sulla *privacy*.

## 2. Protocollo metodologico

### *2.1 Obiettivi della ricerca*

L'obiettivo generale della ricerca è comprendere (a) quante e (b) in che maniera le imprese del campione hanno adottato su base volontaria la nuova normativa ISO/IEC 27701:2019 conseguendo la certificazione di conformità.

Altri obiettivi specifici della ricerca sono i seguenti:

1. rielaborare singolarmente l'esperienza *privacy* e l'impegno RSI delle imprese del campione di riferimento;

2. comprendere come la *privacy policy* viene comunicata agli *stakeholder* delle imprese;

3. verificare se le imprese del campione di riferimento hanno adottato anche altre normative della serie ISO in ambiti diversi alla protezione dei dati conseguendo le relative certificazioni;

4. riscontrare eventuali vantaggi di *marketing* dal lato dell'impresa derivanti da comportamenti socialmente responsabili in materia di *privacy*.

### *2.2 Research questions*

Gli obiettivi della ricerca sopraccitati portano alla definizione delle seguenti domande di ricerca:

RQ1. In seguito alla piena attuazione del GDPR, in che misura e con quali vantaggi le imprese del campione di riferimento hanno adottato su base volontaria la nuova normativa ISO/IEC 27701:2019 per l'implementazione del *Privacy Information Management System* (PIMS)?

RQ2. Quale è la singolare esperienza *privacy* delle imprese del campione di riferimento nell'ambito della propria RSI?

### *2.3 Strumento d'indagine*

Al fine di raggiungere gli obiettivi prefissati e dunque con l'intento di rispondere alle domande di ricerca, si è deciso di ricorrere allo strumento d'indagine della intervista[330]

[330] L'intervista è lo strumento di raccolta delle informazioni più diffuso nelle scienze sociali: secondo alcune stime addirittura il 90% delle ricerche sociali si avvale di informazioni raccolte mediante interviste. V. BRENNER M. (a cura di) (1980), *Social method and social life*, Academic Press Inc, New York, p. 115. L'intervista semi-strutturata (o parzialmente strutturata) è un tipo di intervista in cui vengono poste agli intervistati una serie di domande, sempre le stesse e nello stesso

semi-strutturata a testimoni privilegiati[331], nella fattispecie ai *Data Protection Officer* delle imprese che fanno parte del campione di riferimento. La scelta di considerare i DPO come dei testimoni privilegiati risiede nel fatto che rappresentano i massimi esperti in materia di *privacy* all'interno delle strutture organizzative. In questo modo è stato possibile ricavare dati primari[332] sul fenomeno per poterli successivamente rielaborare qualitativamente. A causa delle ragioni legate alla pandemia da *Covid-19* e data l'impossibilità di potersi incontrare fisicamente, le

ordine per tutti, lasciando libero però l'intervistato di rispondere come crede. È in pratica un'intervista che prevede un insieme fisso e ordinato di domande aperte. Nell'intervista semi-strutturata "l'intervistatore dispone di una lista di temi fissati in precedenza sui quali deve raccogliere tutte le informazioni richieste [con] la facoltà di adattare ai singoli intervistati sia le domande sia l'ordine in cui le pone" v. PITRONE M.C. (1984), *Il sondaggio*, FrancoAngeli Editore, Milano, p. 33. Un'intervista si può considerare parzialmente strutturata anche quando, sebbene la raccolta delle informazioni sia stata operata tramite domande aperte, il ricercatore prevede di organizzare le informazioni stesse in una matrice dei dati. In tal caso l'intervistatore sottopone la domanda in forma aperta, lasciando poi al codificatore il compito di ricondurre la risposta fornita dall'intervistato a una certa categoria in un elenco prestabilito. Cfr. a tal proposito in TRECCANI ENCICLOPEDIA DELLE SCIENZE SOCIALI la voce di FIDELI R. e MARRADI A. (1996), *Intervista*, disponibile *online* al seguente indirizzo *world wide web*: https://www.treccani.it/enciclopedia/intervista_%28Enciclopedia-delle-scienze-sociali%29/.

[331] Per testimoni privilegiati si intende persone che, per l'esperienza acquisita o lo *status* che possiedono, hanno conoscenze particolari sull'oggetto o sul tema della ricerca. Cfr. LOSITO G. (1998), *Sociologia. Un'introduzione alla teoria e alla ricerca sociale*, Carocci Editore, Roma, p. 242; LOSITO G. (1988), *Metodi e tecniche della ricerca sociale empirica sull'emittenza*, in LIVOLSI M. e ROSITI F. (a cura di), *La ricerca sull'industria culturale*, Carocci Editore, Roma, pp. 31-55.

[332] I dati primari sono dati originati per la prima volta dal ricercatore attraverso sforzi diretti ed esperienza, specificamente allo scopo di affrontare il suo problema di ricerca.

interviste sono state condotte telefonicamente. La traccia dei contenuti dell'intervista è stata inoltrata ai DPO con largo anticipo rispetto al riscontro telefonico. Le interviste sono state registrate e in un secondo momento trascritte e riportate in appendice del presente elaborato.

### *2.4 Universo di riferimento e unità d'analisi*

Considerato che la nuova normativa ISO 27701 può essere adottata da qualsiasi impresa indipendentemente dalla dimensione, è altresì fattuale che le grandi imprese trattano generalmente una mole più consistente di dati personali rispetto alle piccole e medie imprese[333]. Per questa ragione

[333] La definizione di PMI è legata a specifici parametri dimensionali individuati espressamente dalla Commissione Europea allo scopo di ottenere una omogeneizzazione fra i vari Stati. A tal proposito, il riferimento è alla raccomandazione n. 2003/361/CE della Commissione, del 6 maggio 2003. Difatti, tale raccomandazione è proprio relativa alla definizione delle microimprese, piccole e medie imprese (2003/361/CE) (in Gazzetta Ufficiale delle Comunità europee L 124 del 20 maggio 2003). Tale raccomandazione è stata recepita dall'ordinamento italiano con decreto del Ministro delle attività produttive del 18 aprile 2005. Pertanto, sono considerate piccole imprese quelle che contestualmente: hanno meno di 50 occupati e un fatturato annuo oppure un totale di bilancio annuo non superiore a 10 milioni di euro. Al contrario, sono medie imprese, invece, quelle che contestualmente hanno meno di 250 occupati e un fatturato annuo non superiore a 50 milioni di euro oppure un totale di bilancio annuo non superiore a 43 milioni di euro. Le imprese che non rientrano nei parametri di cui sopra sono da considerarsi come grandi imprese. All'interno della categoria delle PMI, si definisce microimpresa un'impresa che occupa meno di 10 persone e realizza un fatturato annuo e/o un totale di bilancio annuo non superiori a 2 milioni di euro. In ultimo si definisce grande impresa ogni impresa con 250 o più occupati oppure ogni impresa, anche con meno di 250 occupati effettivi, ma con un fatturato superiore a 50 milioni di euro e un bilancio superiore ai 43 milioni di euro. V. AMANTEA A. (2020),

si è deciso di includere nell'universo di riferimento solo le grandi imprese con sede legale[334] in Italia. In questo contesto, ai fini di una intervista con oggetto lo studio del fenomeno in questione, sono stati contattati via *e-mail* istituzionale i DPO. In totale sono state inoltrate 100 *mail* e, al netto di mancate risposte, declinazioni e defezioni, solo 6 hanno deciso di partecipare alla indagine.

### *2.5 Campione della ricerca*

Il campione della ricerca è dunque costituito da 6 grandi imprese con sede legale in Italia appartenenti a diversi settori economici: agroalimentare (*beverage*), gomma-plastica, automobilistico (*automotive*), telecomunicazioni,

---

*Definizione di PMI: caratteristiche e classificazione delle piccole e medie imprese. Qual è la definizione di PMI e quali caratteristiche si devono rispettare (fatturato e occupati) per rientrare fra le piccole e medie imprese*, Lavoro e Diritti, disponibile *online* al seguente indirizzo *web*: https://www.lavoroediritti.com/soldi-e-diritti/definizione-pmi-piccole-medie-imprese.

[334] La Sede legale (o sede principale, o sede sociale per le società) di una persona giuridica è di regola il luogo in cui dall'atto costitutivo essa risulta avere il centro amministrativo dei propri affari: in genere identifica il luogo in cui si trova l'organizzazione amministrativa dell'impresa. Il concetto di sede legale è l'equivalente del concetto di domicilio per le persone fisiche. In alcuni casi la sede legale può essere ricondotta al luogo di notifica della corrispondenza legale: nella pratica professionale molte società di capitale o cooperative indicano nell'atto costitutivo come sede legale lo studio di un professionista e in tale luogo vengono tenute le riunioni del Consiglio di Amministrazione o anche le assemblee dei soci. Ogni impresa deve avere una ed una sola Sede legale. Nel Registro Imprese ogni impresa è univocamente identificata, a livello nazionale, da un Codice Fiscale e da una Partita IVA: tranne eccezioni CF e PIVA coincidono per le società, mentre sono differenti per le imprese individuali. V. REGISTRO IMPRESE, *I dati ufficiali delle Camere di Commercio*, disponibile *online* al seguente indirizzo *web*: https://www.registroimprese.it/.

sanitario, bancario. Per motivi legati alla delicatezza e sensibilità del tema trattato e a complesse autorizzazioni richieste da parte degli uffici competenti delle imprese stesse, è stato mantenuto l'anonimato in 5 casi su 6 casi, così come espressamente richiesto. Solamente la Banca Popolare di Sondrio ha deciso di palesarsi.

### *2.6 Spazio-tempo*

Le interviste sono state condotte telefonicamente[335] in Italia, tra i mesi di gennaio e settembre[336] 2021.

---

[335] A causa delle disposizioni normative legate alla pandemia da *Covid-19*, le interviste sono state condotte telefonicamente in pieno periodo emergenziale, sebbene la mancanza di un'interazione faccia-a-faccia limiti la "competenza comunicativa" dell'intervistatore e dell'intervistato v. HABERMAS J., *Zur logik der Sozialwissenschaften*, Tübingen, 1967 (tr. it.: *Agire comunicativo e logica delle scienze sociali*, il Mulino, Bologna, 1980). L'intervista telefonica non consente il ricorso a tecniche che comportano strumenti da sottoporre visivamente all'intervistato v. MARRADI A., *L'analisi monovariata*, FrancoAngeli, Milano, 1993, pp. 91-98.

[336] L'intervistatore dispone di meno informazioni per valutare se l'intervistato ha capito davvero la domanda e di conseguenza tenderà a ridurre gli interventi opportuni per chiarire il testo. Non è possibile integrare il resoconto dell'intervista con informazioni relative all'ambiente fisico in cui essa ha luogo e al comportamento non verbale dell'intervistato (v. FREY J.H., *Survey research by telephone*, London 1989, p. 123). Con tutta evidenza, la presenza dell'intervistatore facilita la concessione dell'intervista (v. COLLINS M., SYKES W., *Telephone interviewing on a survey of social attitudes*, in *Survey methods newsletter*, 1985, V, 2, pp. 4-7). Inoltre, siccome l'intervista telefonica non si può protrarre oltre i 20-25 minuti senza irritare l'intervistato e provocare rifiuti di proseguire (v. LAVRAKAS P.J., *Telephone survey methods. Sampling, selection and supervision*, London, 1987, p. 12), l'intervistatore tenderà a porre le domande in modo frettoloso e l'intervistato, cui è lasciato poco tempo per riflettere, a rispondere in modo affrettato.

## 3. Elaborazione e analisi dei dati

Data la peculiarità dello studio e la composizione del campione di riferimento, si è deciso di elaborare e analizzare i dati in maniera qualitativa[337] seguendo un approccio deduttivo[338]. Il processo di elaborazione e analisi dei dati della presente ricerca si avvale (a) del metodo della *Thematic Analysis*[339] per la ricostruzione dei temi

[337] Le procedure qualitative dimostrano un approccio diverso all'indagine scientifica rispetto ai metodi di ricerca quantitativa. L'indagine qualitativa utilizza diversi presupposti filosofici, strategie di indagine e modalità di raccolta dei dati, analisi e interpretazione. Anche se i processi sono simili, le procedure qualitative fanno affidamento su dati di testo e immagine, hanno passaggi unici nell'analisi dei dati e attingono a diverse strategie di indagine. V. CRESWELL J.W. (2009), *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, Thousand Oaks, CA, Sage, Third Edition, p. 173. La ricerca qualitativa è un processo di indagine che si basa sulla comprensione di distinte tradizioni metodologiche di indagine per esplorare un problema sociale o umano. Il ricercatore costruisce una fotografia complessa e olistica, analizza le parole, riporta dettagliatamente il punto di vista degli informatori e conduce lo studio in un *setting* naturale. V. CRESWELL J.W. (1998), *Qualitative inquiry and research design: Choosing among five traditions*, Thousand Oaks, CA, Sage, p. 15.

[338] L'approccio deduttivo implica lo sviluppo di una teoria che viene poi sottoposta a un test rigoroso attraverso una serie di proposte. In quanto tale, è l'approccio di ricerca dominante in ambito delle scienze, dove le leggi presentano la base della spiegazione, consentono l'anticipazione dei fenomeni, prevedere il loro verificarsi e quindi consentire loro di essere controllati. In altri termini, se la ricerca inizia con la teoria, spesso sviluppata dalla lettura della letteratura accademica, e si progetta una strategia di ricerca per testare la teoria, si sta usando un approccio deduttivo. Cfr. SAUNDERS M., LEWIS P., THORNHILL A. (2016), *Research Methods for Business Students*, Pearson Education Limited, London, Seventh edition, pp. 145 – 146.

[339] BRAUN V., CLARKE V. (2006), *Using thematic analysis in psychology*, Qualitative Research in Psychology, Vol. 3, No. 2, pp. 77–101 si riferiscono alla *Thematic Analysis* come un «metodo fondamentale per l'analisi qualitativa». Lo scopo essenziale di questo approccio è cercare

emergenti oggetto di studio e (b) del metodo della *Narrative Analysis*[340] per ciò che concerne la

temi, o modelli, che si verificano in un insieme di dati (come una serie di interviste, osservazioni, documenti o siti *web* oggetto di analisi). L'analisi tematica coinvolge un ricercatore che codifica i suoi dati qualitativi per identificare temi o modelli per ulteriori analisi relativi alla sua domanda di ricerca. L'analisi tematica offre un approccio sistematico ma flessibile e accessibile all'analisi dati qualitativi. È sistematico in quanto fornisce un ordinato e modo logico per analizzare i dati qualitativi. In questo modo, l'analisi tematica può essere utilizzata per analizzare grandi insiemi di dati qualitativi, così come quelli più piccoli, portando a descrizioni ricche, spiegazioni e teorizzazioni. L'analisi tematica è flessibile in quanto non legata a una particolare posizione filosofica. L'analisi tematica può essere utilizzata indipendentemente dal fatto che il ricercatore adotti un approccio deduttivo o induttivo. Cfr. inoltre in merito alla *thematic analysis* SAUNDERS M., LEWIS P., THORNHILL A. (2016), *Research Methods for Business Students*, Pearson Education Limited, London, Seventh edition, p. 579 ss. L'analisi tematica può essere utilizzata per: 1. comprendere quantità spesso grandi e disparate di dati qualitativi; 2. integrare i dati correlati tratti da diverse trascrizioni e note; 3. identificare temi o modelli chiave da un *set* di dati per ulteriori esplorazioni; 4. produrre una descrizione tematica di questi dati; e/o 5. sviluppare e testare spiegazioni e teorie basate su modelli tematici apparenti o relazioni; 6. trarre e verificare le conclusioni.

[340] La *Narrative Analysis* è una raccolta di approcci analitici per analizzare i diversi aspetti della narrativa. Ciò che accomuna questi approcci analitici è la conservazione dei dati forma narrativa. A differenza dell'analisi tematica, in cui i dati originali sono frammentati mediante codifica e quindi assegnati a specifiche categorie, i dati narrativi sono conservati e analizzati come un'intera unità o sequenza narrativa. Nell'Analisi Narrativa è importante preservare i dati nel loro contesto narrativo per mantenere gli elementi sequenziali e strutturali di ogni caso. Le narrazioni testuali possono variare da un segmento di testo o discorso a un'intera storia/esperienza fornita da un narratore. All'interno di questa gamma di possibilità, l'analisi può concentrati sugli estratti delle trascrizioni delle interviste, ognuna delle quali fornisce una breve narrazione su un argomento o un incidente correlato a cui il ricercatore è interessato. Questi estratti tenderanno essere racconti

rielaborazione della singolare esperienza *privacy* delle grandi imprese che hanno aderito allo studio. Data l'esperienza di spicco di una delle imprese facenti parte il campione della ricerca, si è successivamente deciso – nella prospettiva di un ulteriore approfondimento in merito alla adozione del PIMS – di assegnarle maggiore rilevanza mediante (c) il metodo del *Descriptive single case study*[341].

---

che hanno uno scopo chiaro, che racchiudono una situazione, un'azione e un risultato, espresso in una struttura contenente un inizio, un centro e una fine. L'analisi narrativa può utilizzare un approccio di ricerca deduttivo o induttivo. V. SAUNDERS M., LEWIS P., THORNHILL A. (2016), *Research Methods for Business Students*, Pearson Education Limited, London, Seventh edition, p. 600 ss. Cfr. inoltre in merito alla *narrative analysis* MAITLIS, S. (2012), *Narrative analysis*, in SYMON G., CASSELL C. (eds), *Qualitative Organizational Research: Core Methods and Current Challenges*, London, Sage, pp. 492–511; RIESSMAN C.K. (2008), *Narrative Methods for the Human Sciences*, London, Sage.

[341] Il metodo *Case Study* consente a un ricercatore di esaminare da vicino i dati all'interno di un contesto specifico. Nella maggior parte dei casi, il metodo del caso di studio seleziona una piccola area geografica o un numero molto limitato di individui come soggetti di studio. I casi di studio, nella loro vera essenza, esplorano e indagano i fenomeni contemporanei della vita reale attraverso un'analisi contestuale dettagliata di un numero limitato di eventi o condizioni e le loro relazioni. YIN R.K. (1984), *Case Study Research: Design and Methods*, Beverly Hills, Calif, Sage Publications definisce a pag. 23 il metodo del caso di studio di ricerca come una indagine empirica che indaga un fenomeno contemporaneo nel suo contesto di vita reale; quando i confini tra fenomeno e contesto non ci sono chiaramente evidenti; e in cui vengono utilizzate più fonti di prova. In alcuni casi studio viene utilizzato un esame longitudinale approfondito di un singolo caso o evento. L'esame longitudinale fornisce un modo sistematico di osservare gli eventi, raccogliendo dati, analizzando le informazioni e riportando i risultati per un lungo periodo di tempo. In altre parole, il caso di studio è un modo unico di osservare qualsiasi fenomeno naturale che esiste in un insieme di dati. A differenza dell'analisi quantitativa che osserva *pattern* nei dati a livello macro sulla base della frequenza di occorrenza dei fenomeni osservati, i casi di studio

## 4. Presentazione e discussione dei risultati

### *4.1 Cluster tematici*

Il processo di analisi tematica[342] ha consentito di estrapolare dalle trascrizioni delle interviste (v. appendice) i temi rilevanti oggetto di studio e raggrupparli mediante l'utilizzo dei seguenti *cluster*: 1. *Compliance* normativa al *General Data Protection Regulation*; 2. Implementazione del *Privacy Information Management System*; 3. Adozione di altri sistemi per la gestione e sicurezza dei dati; 4. Certificazioni e accreditamenti in materia di protezione dati; 5. Adozione di *standard* normativi della serie ISO; 6.

---

osservano i dati a livello micro. V. inoltre in merito a questo tipo di metodo YIN R.K. (1981), *The Case Study Crisis: Some Answers*, Administrative Science Quarterly, Vol. 26, No. 1, pp. 58-65. Esistono diverse categorie di casi di studio. YIN (1984), op. cit., annota tre categorie, vale a dire casi di studio (a) esplorativi, (b) descrittivi ed (c) esplicativi. Il caso di studio presentato è di tipo descrittivo, dunque impostato per descrivere i fenomeni naturali che si verificano all'interno dei dati in questione. L'obiettivo prefissato dal ricercatore è descrivere i dati man mano che si verificano. MCDONOUGH J. e MCDONOUGH S. (1997), *Research Methods for English Language Teachers*, London, Arnold, suggeriscono che i casi di studio descrittivi possono essere in forma narrativa. V. per una lettura organica in merito al metodo di ricerca del caso studio ZAINAL Z. (2007), *Case study as a research method*, Jurnal Kemanusiaan, bil. 9.

[342] L'analisi tematica offre un approccio sistematico all'analisi qualitativa dei dati che è accessibile e flessibile. Rispetto ad alcuni approcci qualitativi, non è eccessivamente prescrittivo sull'applicazione delle sue procedure analitiche. Come approccio generico all'analisi qualitativa dei dati, è adatto all'uso con diverse strategie di ricerca qualitativa, dove non si sta seguendo una precisa strategia che prescrive precise procedure analitiche. V. SAUNDERS M., LEWIS P., THORNHILL A. (2016), op. cit., p. 587. Il processo si compone delle seguenti fasi: 1. Acquisizione familiarità con i dati; 2. Codifica dei dati; 3. Ricerca dei temi e riconoscimento delle relazioni; 4. Affinazione dei temi e proposte.

Altri comportamenti e pratiche socialmente responsabili; 7. Modalità di comunicazione della *privacy policy*; 8. Vantaggi di *marketing* derivanti da comportamenti socialmente responsabili in materia di *privacy*. Di seguito sono riportati ulteriori approfondimenti per ciascun raggruppamento tematico.

Compliance normativa al GDPR

Tutte le imprese del campione si dichiarano *compliant* al GDPR, fermo restando che la *compliance* non è un esercizio statico. *Compliance* significa conformità normativa. Essere *compliant* quindi significa essere conformi. In ambito GDPR, essere *compliant* significa rispettare princìpi e regole previsti dal Regolamento europeo 2016/679 con un atteggiamento proattivo, non passivo di fronte al dettato normativo, e quindi agire sempre e prima di tutto con responsabilizzazione e responsabilità. Nel caso di mancata conformità alle disposizioni coercitive, lo stesso GDPR prevede pesanti sanzioni in cui le imprese possono incorrere.

Implementazione del PIMS

Data la sua natura volontaria, solamente una impresa del campione ha adottato la nuova normativa ISO/IEC 27701:2019 con conseguente implementazione del *Privacy Information Management System* (PIMS) ottenendo la relativa certificazione di conformità. Vi sono tuttavia due casi su cui porre l'attenzione: nel primo, l'eventuale avvio di un processo di adozione e certificazione ISO/IEC 27701:2019 verrà valutato dall'impresa a seguito dell'ottenimento della certificazione ISO 27001:2013 già in programma, mentre nell'altro l'adozione della nuova estensione ISO per l'implementazione di un PIMS rientra nei punti programmatici dei futuri esercizi aziendali. Nonostante la maggior parte delle imprese del campione

non si sia (ancora) dotata di un PIMS, ognuna di queste rispetta scrupolosamente quanto previsto dal GDPR.

Adozione di altri sistemi per la gestione e sicurezza dei dati

Il Sistema di Gestione della Sicurezza delle Informazioni (ISMS - ISO/IEC 27001) si conferma essere il più utilizzato; difatti, metà delle imprese del campione – oltre la *compliance* al GDPR – lo sta già adottando. Una impresa ha in programma entro il 2022 l'adozione della normativa ISO/IEC 27001, indispensabile per l'eventuale passaggio alla ISO/IEC 27701 per l'implementazione del PIMS. In un altro caso, una impresa adotta la ISO 27001 combinata con *standard* di gestione *privacy* BS 10012:2017, elaborato e promosso dalla Organizzazione Britannica di Standardizzazione (*British Standards Institution*), che rappresenta un valido strumento per la gestione aziendale degli aspetti organizzativi e prescrittivi previsti dal Regolamento UE 2016/679. Una impresa sta estendendo il proprio ISMS in PIMS abbracciando la nuova normativa ISO 27701. In altri due casi, una impresa si è dotata di un sistema di gestione *privacy* autoprodotto con supporto di consulenti esterni e collaborazioni con *cybersecurity team* mentre l'altra, tramite la funzione *Group Privacy and Data Protection* (GPDP), ha implementato un *tool* che permette di gestire e tracciare le principali attività richieste, al fine di essere in grado di dimostrare efficacemente la *compliance* al GDPR.

Certificazioni e accreditamenti in materia di protezione dati

Solo 2 imprese su 6 hanno ottenuto una certificazione in materia di protezione dei dati personali (BS10012 e ISO27701). Nella metà dei casi (3 su 6), invece, è stata comunque ottenuta una certificazione in materia di sicurezza delle informazioni. La DNV GL (*Det Norske Veritas),* uno dei principali enti di certificazione a livello

mondiale, in seguito ai dovuti accertamenti, ha riconosciuto alle imprese il mantenimento delle certificazioni relative ai temi di sicurezza delle informazioni (ISO/IEC 27001) e protezione dei dati personali (ISO/IEC 27701).

Adozione di standard normativi della serie ISO

A seconda del settore economico di riferimento e dunque a specifiche esigenze, tutte le imprese del campione hanno mantenuto la *compliance* agli *standard* normativi internazionali della serie ISO e confermato così il loro impegno anche in ambiti differenti alla protezione dei dati. Nel dettaglio, altre normative della serie ISO adottate dalle imprese che hanno aderito alla ricerca sono le seguenti: Sistemi di gestione della qualità – ISO 9001 (5 su 6); Sistemi di gestione per la salute e la sicurezza sul lavoro – ISO 45001 (5 su 6); Sistemi di gestione ambientale – ISO 14001 (5 su 6); Sistemi di gestione dell'energia – ISO 50001 (1 su 6); Sistemi di gestione per la sicurezza alimentare – ISO 22000 (1 su 6); Requisiti generali per la competenza dei laboratori di prova e di taratura – ISO/IEC 17025 (1 su 6). Si segnala inoltre – al di fuori del contesto delle certificazioni ISO – l'adozione della SA 8000 – 'Responsabilità sociale' da parte di una sola impresa.

Altri comportamenti e pratiche socialmente responsabili

Tutte le imprese si impegnano anche in ambiti diversi alla protezione dei dati personali, adottando politiche socialmente responsabili. Nella totalità dei casi, le politiche vengono sostanzialmente rendicontate nel bilancio sociale o di sostenibilità oppure tramite *report* e i principi sono dichiarati nel codice etico aziendale. La responsabilità sociale delle imprese oggetto di studio si articola principalmente in campo ambientale, lotta alla corruzione, risorse umane, rispetto dei diritti umani e pari opportunità,

sicurezza sul lavoro, trasparenza, educazione e innovazione digitale. Con riferimento ad altre pratiche socialmente responsabili in materia di protezione dei dati, si segnalano: 1. l'istituzione di numerose attività di *training* e *awareness* nell'ambito delle attività progettuali, mediante l'istituzione di corsi di formazione a neoassunti e più in generale a tutto il personale; 2. specifiche attività di monitoraggio con tutti i responsabili aziendali nell'ambito della tenuta del registro dei trattamenti nonché attività di verifica tramite un sistema di autovalutazione di tutti i fornitori nominati responsabili del trattamento; 3. collocazione del ruolo del DPO all'interno della Funzione di Conformità creando un'unità organizzativa apposita di Presidio Operativo all'interno dell'Ufficio Gestione e Protezione dei dati; 4. l'istituzione di un sistema di *governance*, *risk management* e *compliance* che consente di tenere sotto controllo l'intera filiera del trattamento dei dati, valutando in maniera analitica il livello di conformità di ciascun sistema coinvolto.

Modalità di comunicazione della privacy policy

Le modalità di comunicazione delle *privacy policy* dipendono sostanzialmente dal canale di raccolta dei dati personali e dalla tipologia di destinatari e avvengono ogni qualvolta vengono trattati dati personali, mediante il rilascio della informativa *privacy* (art. 13 GDPR). Non vi è tuttavia una modalità *standard* di comunicazione ma è possibile constatare che le imprese del campione privilegiano tendenzialmente modalità di comunicazione di tipo digitale o comunque dematerializzate. Gli strumenti di comunicazione dell'impegno alla *privacy* sono molteplici e spaziano dalle comuni circolari aziendali alle relazioni del DPO, dalla informativa annuale alle infografiche e *videoclip online*, dal sito *web* aziendale al bilancio sociale o ai *report* di sostenibilità. In un caso, la

*privacy* è addirittura considerata parte integrante della *responsibility*, una delle quattro aree del modello di sostenibilità aziendale.

Vantaggi di marketing derivanti da comportamenti socialmente responsabili in materia di privacy

Data la difficile quantificazione e l'impossibilità di una misurazione, i vantaggi e i benefici di *marketing* derivanti dall'impegno e dall'esperienza *privacy* delle imprese sono frutto di una valutazione soggettiva dei propri DPO. Nella totalità dei casi, i DPO hanno ritenuto che l'adozione di comportamenti socialmente responsabili in materia di *privacy* abbiano generato vantaggi di *marketing* dal lato impresa. Tali vantaggi sono vari e trascendono il solo ambito del *marketing*. In generale, i comportamenti responsabili hanno avuto e continuano ad avere ricadute positive sia in termini di competitività, sia in termini di etica d'impresa e consapevolezza interna dell'importanza della *privacy*. Tutto ciò che può rispondere a valori etici, difatti, può portare solamente benefici ai processi aziendali e allo sviluppo. Evitare il danno d'immagine per eventuali *data breach* costituisce già un obiettivo e dunque un vantaggio d'impresa. L'impegno responsabile e sostenibile alla *privacy* è una delle leve strategiche per la crescita e per la definizione delle politiche e strategie aziendali. Dotarsi di un apposito sistema informativo di gestione della clientela e del relativo *marketing* (cd. CRM) utilizzato nel rispetto della normativa *privacy* aiuta a perseguire i propri obiettivi aziendali. Un approccio alla responsabilità sociale d'impresa trasparente ed integrato con il *core business* si verifica ogni qualvolta l'impresa adotta pratiche commerciali corrette ed improntate al principio della trasparenza, della chiarezza, della semplicità e della correttezza verso i clienti nell'ottica di un *marketing* socialmente responsabile.

### *4.2 L'esperienza privacy delle imprese*

Il processo di analisi narrativa ad approccio tematico[343] ha consentito di ricostruire e organizzare separatamente la singolare esperienza *privacy* delle imprese per soddisfare gli obiettivi e rispondere alle domande della ricerca.

Impresa nr. 1 (settore agroalimentare – *beverage*)

La multinazionale opera nel settore alimentare ed è attiva, in particolare, nella produzione di bevande analcoliche e alcoliche, dove si posiziona tra i *leader* mondiali. L'impresa si presenta conforme a tutte le disposizioni coercitive in materia di protezione dei dati personali previste dal GDPR ma non si è dotata del nuovo *standard* normativo ISO/IEC 27701:2019 per l'implementazione del PIMS. Al contempo, ha però definito una serie di *policy* per

[343] Vi sono sostanzialmente due approcci utilizzati nell'analisi narrativa. Si tratta della (a) analisi narrativa tematica e della (b) analisi narrativa strutturale, cfr. MAITLIS (2012), op. cit.; RIESMANN (2008), op. cit. La presente ricerca segue l'approccio della analisi narrativa tematica. Lo scopo dell'analisi narrativa tematica è identificare i temi analitici all'interno delle narrazioni. Questo approccio si concentra sul contenuto di una narrazione, piuttosto che al modo in cui è strutturato. In questo approccio l'enfasi è quindi su cosa tratta la narrazione piuttosto che su come è costruita. L'analisi narrativa tematica può essere utilizzata per analizzare delle narrazioni individuali o multiple, per poi poterle correlare. L'analisi di più narrazioni inizia analizzando ogni narrazione separatamente o, in alternativa, lavorando su tutte le narrazioni allo stesso tempo. Nell'analizzare più narrazioni separatamente, l'enfasi iniziale è posta sull'analisi approfondita di ogni singola narrazione, prima ancora del confronto dei risultati. Diverse narrazioni vengono analizzate individualmente per svariati motivi, tra cui quello di illustrare come le variazioni di contesto influiscano sulle azioni intraprese e sui risultati registrati o per illustrare come le differenze nelle azioni intraprese e nei risultati registrati può variare nonostante le somiglianze contestuali, e per spiegare il perché. V. SAUNDERS M., LEWIS P., THORNHILL A. (2016), op. cit., pp. 601-602.

la gestione dei requisiti del GDPR e ha anche implementato un *tool* che permette di gestire e tracciare le principali attività richieste, al fine di essere in grado di dimostrare efficacemente la *compliance* al Regolamento UE 2016/679. Tramite la funzione *Group Privacy and Data Protection* (GPDP) ha gestito il progetto di adeguamento al nuovo Regolamento europeo. È stato nominato un *Data Protection Officer* ed è stato inoltre definito un modello organizzativo in materia di protezione dei dati personali, identificando ruoli e responsabilità. Nell'ambito delle attività progettuali, sono state inoltre eseguite numerose attività di *training* e *awareness*. L'impresa non si è dotata di altri sistemi per la protezione dei dati né ha ottenuto certificazioni in materia. La multinazionale ha mantenuto la *compliance* agli *standard* internazionali di sicurezza alimentare ottenendo la ISO22000 e ha definito un programma di certificazioni per migliorare le *performance* nei prossimi anni. Con riferimento alle certificazioni ambientali, ha ottenuto la ISO14001 e ISO50001 e la certificazione ISO45001 in ambito salute e sicurezza. Si è impegnata altresì in ambito sociale, ambientale, lotta alla corruzione, risorse umane, rispetto dei diritti umani e tutte le politiche sono menzionate nei *report* di sostenibilità, come pure la totalità dell'impegno *privacy*. Ha ritenuto necessario definire un progetto strutturato dedicato alla sostenibilità, con l'obiettivo di diffondere internamente la cultura della responsabilità d'impresa, realizzare progetti a supporto delle persone e condividere con gli *stakeholder* i risultati ottenuti comunicati generalmente *online*. Il percorso di sostenibilità è stato avviato ufficialmente nel 2011, con l'ambizione di rendere la sostenibilità una delle leve strategiche per la crescita e per la definizione delle politiche aziendali. Per ciò che concerne i vantaggi di *marketing* derivanti da comportamenti e pratiche socialmente responsabili in ambito protezione dati, si è

ritenuto difficile darne una precisa quantificazione ma, ciononostante, sicuramente l'impresa ne ha beneficiato dato il suo impegno.

Impresa nr. 2 (settore gomma–plastica)

L'impresa è controllata al 100% da una società per azioni multinazionale che opera nel settore della gomma-plastica. In particolare, è specializzata nella produzione di pneumatici per automobili, motocicli e biciclette. Si dichiara conforme a tutte le disposizioni in materia *privacy* previste dal nuovo Regolamento europeo e puntualizza che la *compliance* al GDPR non è un esercizio statico. Non ha adottato la nuova ISO 27701 ma si è approcciata alla combinazione sinergica ISO 27001 e BS 10012, anche se non in tutti i Paesi in cui opera, e ha ottenuto la certificazione in materia di *data protection*, diversa dalla certificazione GDPR, in quanto il meccanismo di richiesta e attribuzione di tali certificazioni e accreditamenti è ancora in corso di definizione sia a livello italiano che europeo. Svolge comunque un'intensa attività nel campo dei Sistemi di Gestione, avvalendosi di questi strumenti per migliorare la qualità, l'efficacia e l'efficienza dei propri processi, nonché al fine di perseguire un'ulteriore riduzione degli impatti sulla salute dei dipendenti, sulle condizioni di sicurezza del lavoro e sull'ambiente esterno: ha ottenuto così le certificazioni di qualità ISO 9001 e ISO/IEC 17025, la certificazione ISO 14001 per l'ambiente e infine la ISO 45001 per il sistema salute e sicurezza. Nel Codice etico di Gruppo sono rappresentati i principi generali di trasparenza, correttezza e lealtà cui si ispira lo svolgimento e la conduzione degli affari. Esso indica gli obiettivi e i valori informatori dell'attività d'impresa, con riferimento ai principali *stakeholders* con i quali si trova quotidianamente a interagire. Più in generale, le modalità di comunicazione delle *privacy policy* dipendono dal canale di raccolta dei

dati personali e dalla tipologia di destinatari e non vi è tuttavia una modalità *standard* di comunicazione. La società privilegia tendenzialmente modalità di comunicazione di tipo digitale o comunque dematerializzate. I vantaggi derivanti da comportamenti socialmente responsabili in materia di *privacy* sono vari e trascendono il solo ambito del *marketing*. In generale, tali comportamenti hanno avuto e continuano ad avere ricadute positive sia in termini di competitività della società, sia in termini di etica d'impresa e consapevolezza interna dell'importanza della *privacy*.

Impresa nr. 3 (settore automobilistico – *automotive*)

L'impresa è una produttrice italiana di veicoli a due ruote a motore e veicoli commerciali. Opera nel settore utilizzando vari *brand*. Si presenta conforme pienamente al GDPR, ma non ha ancora adottato la nuova ISO 27701, in quanto di natura volontaria. L'eventuale avvio di un processo di certificazione e adozione della ISO/IEC 27701:2019 verrà valutato a seguito dell'ottenimento della certificazione ISO 27001, prevista entro il 2022. Per questo motivo, non ha ancora ottenuto alcuna certificazione in materia di protezione dati. Il Gruppo vanta sistemi di gestione dell'ambiente, della qualità e della sicurezza del lavoro di eccellenza in tutti i suoi siti produttivi. Il Gruppo è dunque certificato ISO 9001 – Sistemi di gestione della qualità; ISO 14001 – Sistemi di gestione ambientale e ISO 45001 – Sistemi di gestione per la salute e la sicurezza sul lavoro. L'impresa ha adottato altri comportamenti e pratiche socialmente responsabili in vari ambiti: in ambito risorse umane, tramite una corretta gestione delle diversità e un'offerta di pari opportunità a entrambi i sessi; in ambito sicurezza sul lavoro, il Gruppo ha intrapreso azioni concrete finalizzate a consentire una evoluzione continua per un lavoro più sicuro che parte dalla valutazione degli

aspetti relativi alla sicurezza dell'ambiente di lavoro e ai relativi strumenti, fin dalle fasi di definizione delle nuove attività, o nella revisione di quelle esistenti e comportamenti più sicuri attraverso la formazione, informazione e sensibilizzazione di tutti i lavoratori, per consentire loro di svolgere i propri compiti in sicurezza e di assumere la responsabilità in materia di salute e sicurezza sul lavoro; in ambito ambientale, il Gruppo ha definito una specifica struttura organizzativa preposta al perseguimento degli obiettivi di sostenibilità ambientale dei propri siti produttivi. L'impresa comunica la propria *privacy policy* attraverso sito *web*, bilancio sociale e ogni qual volta vengano trattati dati personali. Il DPO ha tenuto a sottolineare che il *business* aziendale relativo a settore *automotive* non rientra tra quelli ad elevata presenza e gestione di dati personali (es. come istituti di credito, compagnie telefoniche). Conseguentemente la società, che comunque tratta dati personali, si è dotata di un apposito sistema informativo di gestione della clientela e del relativo *marketing* (cd. CRM) utilizzato nel rispetto della normativa *privacy*. Come indicato nell'ultimo *Corporate Social Responsibility report* pubblicato, non si registrano, infine, nel corso del 2020, casi di reclami relativi a violazioni della *privacy* o perdita dei dati dei clienti. Inoltre, al 31 dicembre 2020 non risultano sanzioni riferite a non conformità a leggi e regolamenti, inclusi leggi e regolamenti di natura ambientale, attività di *marketing*, pubblicità, promozione, sponsorizzazione, fornitura ed utilizzo dei propri prodotti.

Impresa nr. 4 (settore telecomunicazioni)

L'impresa è operante nel settore delle telecomunicazioni, nata come *joint venture* paritaria tra due gruppi in seguito alla fusione per incorporazione. La politica aziendale sul tema della *privacy* e sicurezza dei dati mira innanzitutto a garantire la conformità normativa, con riferimento al

contesto legislativo sia nazionale che comunitario, tenendo conto dell'introduzione del nuovo GDPR e anche dell'introduzione della nuova normativa sui temi della *cybersecurity*. L'adozione della nuova ISO 27701 per l'implementazione di un PIMS rientra nei punti programmatici dei prossimi esercizi aziendali e la ISO/IEC 27001 per la Sicurezza delle Informazioni viene già adottata da diversi anni. Grazie anche ai processi di armonizzazione avvenuti negli anni precedenti, l'azienda adotta oggi un sistema di G*overnance, Risk Management e Compliance* (eGRC) che consente di tenere sotto controllo l'intera filiera del trattamento dei dati, valutando in maniera analitica il livello di conformità di ciascun sistema coinvolto. Periodicamente, sono effettuate delle specifiche attività di monitoraggio con tutti i responsabili aziendali nell'ambito della tenuta del registro dei trattamenti nonché attività di verifica tramite un sistema di autovalutazione di tutti i fornitori nominati responsabili del trattamento. DNV GL, uno dei principali enti di certificazione a livello mondiale, ha infatti riconosciuto all'azienda il mantenimento delle certificazioni relative ai temi di Sicurezza delle Informazioni (ISO/IEC 27001). L'azienda conferma il proprio impegno nell'integrare la sostenibilità con la gestione del *business*, per contribuire alla realizzazione degli obiettivi dell'Agenda 2030. In ambiti differenti alla protezione dei dati personali, l'azienda ha ottenuto certificazioni relative ai temi di Salute e Sicurezza sul Lavoro (ISO 45001), Ambiente (ISO 14001), Responsabilità sociale (SA 8000), Qualità (ISO 9001). Fin dalla nascita, l'azienda ha rendicontato volontariamente gli impatti sociali e ambientali. L'approccio dell'azienda alla responsabilità d'impresa si basa sostanzialmente su quattro punti alla base del rapporto dell'azienda con i propri *stakeholder* e delle attività di responsabilità sociale e ambientale: 1. trasparenza e approccio a 360°; 2. efficienza

nell'uso delle risorse; 3. educazione e innovazione digitale; 4. partecipazione e coinvolgimento nella comunità. La *privacy* viene considerata parte integrante della *responsibility*, una delle quattro aree del modello di sostenibilità aziendale. La *privacy policy* viene comunicata nel bilancio di sostenibilità e ogni qualvolta vengono trattati dati personali, principalmente *online*. La corretta gestione dei dati aziendali e dei clienti da parte dell'azienda è un requisito indispensabile per la sua credibilità sul mercato. L'azienda adotta pratiche commerciali corrette ed improntate al principio della trasparenza, della chiarezza, della semplicità e della correttezza verso i clienti nell'ottica di un *marketing* responsabile. L'azienda crede in un approccio alla responsabilità sociale d'impresa trasparente ed integrato con il *core business*. Il tema della *privacy* e della sicurezza dei dati è molto sensibile per l'azienda, che custodisce un'enorme quantità di informazioni relative ai clienti e alle loro abitudini e preferenze. L'eventualità di una significativa perdita di dati comporterebbe per l'azienda dei rischi rilevanti sotto il profilo reputazionale, economico e operativo. Con questa consapevolezza l'azienda attua, quindi, tutte le misure necessarie a presidiare accuratamente la sicurezza dei dati, delle informazioni così come il rispetto della *privacy* e delle recenti normative in tema di *cybersecurity*, nell'interesse dei clienti e dell'azienda stessa. Inoltre, l'azienda si prefigge di prevenire eventuali perdite o danneggiamenti dei dati gestiti, limitare i danni e ripristinare la normale operatività aziendale nel più breve tempo possibile, nel caso di eventuali incidenti.

Impresa nr. 5 (settore sanitario)

L'impresa è uno dei più grandi gruppi ospedalieri privati italiani, con centri diagnostici e ospedali situati nel nord Italia. Il gruppo si presenta conforme a tutte le disposizioni

coercitive previste dal GDPR, nell'ottica di un continuo aggiornamento. Dotata di un sistema di gestione *privacy* autoprodotto con supporto di consulenti esterni e collaborazioni con *cybersecurity team*, non ha adottato né ISO 27001 né ISO 27701 e quindi è sprovvista di certificazioni in materia di sicurezza e protezione dei dati. L'impresa è attenta in ambito sociale, in particolare in ambiente, sicurezza sul lavoro e anticorruzione e ha ottenuto le certificazioni ISO 9001, ISO 14001 e ISO 45001. La *privacy policy* viene comunicata principalmente tramite l'informativa *privacy*, canali *online*, relazioni del DPO e informativa annuale. Inoltre, sul tema della protezione dati, sono stati istituiti dei corsi di formazione in presenza con l'aiuto di infografiche e *videoclip*, e da remoto, avvalendosi della rete *Intranet*. I vantaggi di *marketing* non sono quantificabili in quanto non misurati, ma sicuramente ottenuti. Evitare il danno d'immagine per eventuali *data breach*, secondo il DPO, costituisce già un obiettivo e dunque un vantaggio d'impresa.

Impresa nr. 6 (settore bancario)

La Banca Popolare di Sondrio, società cooperativa per azioni, è capogruppo dell'omonimo gruppo bancario. Già da diversi anni, la banca dispone di un articolato *framework* integrato di sicurezza e gestione dei rischi ICT (*information and communications technology*) adottato dai sistemi informativi fortemente basato sugli *standard* ISO 27001 e 27701. In particolare, lo *standard* ISO 27701 per l'implementazione del *Privacy Information Management System* è stato certificato ufficialmente nel dicembre 2020, in seguito agli accertamenti condotti dall'ente di certificazione DNV (*Det Norske Veritas*) per l'ambito Sistemi Informativi. Banca Popolare di Sondrio si presenta conforme a tutte le disposizioni coercitive previste dal *General Data Protection Regulation* e a sostegno e

presidio di tale tema ha adottato sia provvedimenti organizzativi, collocando internamente il ruolo di DPO all'interno della Funzione di Conformità, creando un'unità organizzativa apposita di Presidio Operativo (cd. Presidio Operativo di protezione dei dati personali) all'interno dell'Ufficio Gestione e Protezione dei dati, sia provvedimenti operativi, con l'emissione da parte del Consiglio di Amministrazione nel 2018 dell'articolato "Regolamento in materia di Protezione dei Dati Personali" correlato di specifici modelli operativi, organizzativi e di controllo, a copertura dei vari aspetti della tematica (es. contratti e nomine a responsabile esterno, diritti degli interessati, registro dei trattamenti). Sul tema è stato effettuato un piano continuo di formazione che prevede corsi ai neoassunti, corsi a tutto il personale (tramite corsi online interni) e corsi su aspetti specifici (es. registro dei trattamenti e nomine a responsabile del trattamento esterno) erogati alle figure d'interesse. Su base volontaria le varie divisioni della banca operano per ottenere le certificazioni che ritengono utili, come la ISO 9001 per il sistema gestione della qualità. La banca è tradizionalmente impegnata nel perseguimento di *standard* qualitativi elevati, con l'obiettivo di massimizzare l'efficienza e soddisfare al meglio la clientela. Inoltre, in conformità al decreto legislativo nr. 254/2016, ha redatto la dichiarazione consolidata di carattere non finanziario (DNF), pubblicata sul sito istituzionale della stessa. Nello specifico, la DNF ha il fine di assicurare la comprensione delle *policy*, del modello organizzativo, dei rischi e degli indicatori di *performance* e dei relativi risultati del Gruppo rispetto, in particolar modo, agli aspetti sociali e attinenti alla gestione del personale, alla lotta contro la corruzione attiva e passiva e al rispetto dei diritti umani. In aggiunta, la banca ha da tempo adottato il "modello di organizzazione, gestione e controllo" ai sensi del decreto legislativo n. 231 dell'8

luglio 2001 e successive modificazioni e integrazioni e ha recentemente aggiornato anche il codice etico aziendale, allineando i comportamenti attesi in relazione al rispetto delle più recenti normative. La comunicazione della *privacy policy* avviene attraverso i normali mezzi di comunicazione delle prassi operative (es. circolari aziendali) e mediante il sito *web* della banca stessa. È difficile poter misurare eventuali vantaggi di *marketing* a seguito di comportamenti socialmente responsabili in materia di *privacy*, tuttavia, a loro avviso, tutto ciò che può rispondere a valori etici, a cui la banca crede e imposta da sempre la propria attività, può portare solamente benefici ai processi aziendali e allo sviluppo dell'istituto.

### *4.3 Caso di studio d'eccellenza: Banca Popolare di Sondrio e l'implementazione del PIMS*

Banca Popolare di Sondrio merita certamente un paragrafo integrativo che meglio descrive il singolo caso studio[344]. Fondata nel 1871, la Banca Popolare di Sondrio è una delle prime banche popolari italiane ispirate al movimento popolare cooperativo del credito. La banca presta alla propria clientela (famiglie, professionisti, imprese di

[344] Un caso di studio descrittivo è una storia concernente una situazione del mondo reale che è stata affrontata da persone o gruppi. Include un resoconto conciso ma completo dei fatti della situazione e un commento di esperti che aiuta il pubblico a comprendere le cause di una problematica, i vantaggi di una soluzione, i risultati di una implementazione, le lezioni apprese e le connessioni a teorie, concetti, politiche e strumenti rilevanti per la situazione in esame. I casi descrittivi comprendono materiali e non pubblicazioni di ricerca. Il contenuto presentato è stato ricavato mediante una rassegna stampa e del *web* del materiale esistente e disponibile sul tema. Cfr. MILLS A. J., DUREPOS G., WIEBE E. (2010), *Descriptive Case Study* in *Encyclopedia of Case Study Research,* SAGE Publications, Thousand Oaks, CA.

piccole e grandi dimensioni, enti pubblici, ecc.) servizi in grado di soddisfare qualsiasi esigenza bancaria, finanziaria e assicurativa. Collateralmente all'attività primaria la banca promuove iniziative a sfondo culturale: fra queste spiccano, per prestigio e risonanza, l'organizzazione di eventi legati al nome di eminenti personaggi e una raffinata attività editoriale[345]. Banca Popolare di Sondrio ha ottenuto, tra le prime banche in Italia, la certificazione ISO/IEC 27701 dall'ente di certificazione *leader* a livello mondiale DNV GL per il Servizio Organizzazione Sistemi Informativi[346]. Da sempre particolarmente sensibile e attenta alla tutela dei dati dei propri clienti, con questa certificazione Banca Popolare di Sondrio rafforza il proprio *commitment* a implementare i più stringenti requisiti internazionali in materia di gestione della sicurezza delle informazioni e, in particolare, di tutela della *privacy* delle informazioni personali. In un mondo sempre più connesso, i temi della *personal data protection* e della tutela della *privacy* rivestono un ruolo prioritario per ogni organizzazione; ancor più per quelle che operano nel settore bancario. Banca Popolare di Sondrio ha deciso di

[345] Cfr. il sito *web* ufficiale della BANCA POPOLARE DI SONDRIO al seguente indirizzo *online*: https://www.popso.it/, in particolare la sezione "Chi siamo".

[346] DNV GL - *Business Assurance* DNV GL è *leader* nella gestione del rischio e uno dei principali enti di certificazione a livello mondiale. Attraverso i servizi di certificazione dei sistemi di gestione, dei prodotti e delle catene di fornitura supporta le aziende di diversi settori, incluso il *food & beverage*. Mette a disposizione le proprie competenze tecniche, digitali e di settore per permettere alle aziende di dimostrare la propria conformità agli *standard*, prendere decisioni migliori e agire. Le loro soluzioni digitali integrate consentono alle aziende e ai *partner* di raggiungere in modo efficiente un'elevata integrità della *supply chain*. Con origini che risalgono al 1864 e una presenza in oltre 100 Paesi, affiancano i clienti nello sviluppo di *performance* di *business* sostenibili e nella creazione di fiducia da parte degli *stakeholder*.

aderire ad uno degli *standard* di riferimento tra i più rigorosi, per regolamentare la gestione dei dati personali. I requisiti e i controlli contemplati dalla ISO/IEC 27701, non soltanto tengono in considerazione la normativa tecnica internazionale vigente (ISO/IEC 27001, ISO/IEC 27002, il *privacy framework* ed i principi espressi nella ISO/IEC 29100, ISO/IEC 27018, ISO/IEC 29151), ma fanno altresì esplicito riferimento alla specifica normativa comunitaria in materia di protezione dei dati personali (GDPR), indicando in modo chiaro ed analitico gli adempimenti che competono al titolare e al responsabile del trattamento. Conseguentemente, i modelli di valutazione e presidio dei rischi della sicurezza dei sistemi informativi potranno essere integrati e correlati con quelli dedicati ai rischi *privacy*, tenendo ovviamente conto delle specificità introdotte dal GDPR[347]. Massimo Alvaro, *Managing Director Italy & Adriatics* di DNV GL ha commentato: "le nostre verifiche hanno dato esito pienamente soddisfacente, confermando il livello di implementazione da parte di Banca di Sondrio di un sistema atto a garantire adeguati livelli di riservatezza, integrità e disponibilità delle informazioni. La certificazione ISO/IEC 27701 sottolinea inoltre quanta attenzione la Banca ponga nella sicurezza delle informazioni personali gestite, incluse quelle dei clienti finali"[348]. Giampiero Raschetti, responsabile della sicurezza dei sistemi informativi di

[347] Cfr. sito ufficiale della BANCA POPOLARE DI SONDRIO disponibile al seguente indirizzo *world wide web*, in particolare alla voce "Sicurezza *online* – Certificazioni di sicurezza": https://www.popso.it/servizi-online/sicurezza/certificazione-sicurezza-iso27001.

[348] REDAZIONE PRIMA LA VALTELLINA (2021), *Certificazione ISO/IEC 27701 alla Banca Popolare di Sondrio per la tutela della privacy*, disponibile *online* al seguente indirizzo *web* della redazione locale valtellinese: https://primalavaltellina.it/economia/certificazione-iso-iec-27701-alla-banca-popolare-di-sondrio-per-la-tutela-della-privacy/.

Banca Popolare di Sondrio, ha aggiunto: "aver ottenuto la certificazione ISO/IEC 27701 da parte di DNV GL non è un punto di arrivo per la nostra organizzazione. La salvaguardia della sicurezza delle informazioni dei nostri clienti è un dovere imprescindibile per chi opera in un settore come il nostro. Un aspetto sul quale lavoriamo quotidianamente con il massimo impegno, per offrire elevati livelli di garanzia e favorire la proposizione di servizi competitivi nel mercato finanziario"[349]. La certificazione ha validità 21 dicembre 2020 - 20 dicembre 2023 per il campo applicativo "Sistema di gestione della sicurezza delle informazioni e dei dati personali relativo alla progettazione, sviluppo e mantenimento dei servizi di *online banking*, di strumenti e di servizi a supporto della progettazione e dello sviluppo applicativo e della gestione dei sistemi e delle reti informatiche siti nella *Server Farm*"[350]. La validità dell'attestato è legata a quella del certificato ISO/IEC 27001:2013 e soggetta alla effettuazione delle verifiche periodiche di mantenimento o di rinnovo della validità come previsto dalle regole di accreditamento ISO/IEC 27006:2015.

---

[349] REDAZIONE DNV (2021), *ISO/IEC 27701 alla Banca Popolare di Sondrio per la tutela della privacy*, disponibile *online* al seguente indirizzo *web* ufficiale: https://www.dnv.it/news/iso-iec-27701-alla-banca-popolare-di-sondrio-per-la-tutela-della-privacy-194859.
Cfr. inoltre per ulteriori approfondimenti il video caricato sulla piattaforma YOUTUBE, *Insights Talk - Parliamo di gestione della privacy con Giampiero Raschetti, di Banca Pop Sondrio*, disponibile al seguente indirizzo *web*: https://www.youtube.com/watch?v=Kc3x3u5G_Fk.

[350] Per visualizzare in formato *Portable Document Format* (PDF) il certificato del sistema di gestione ISO/IEC 27701:2019 (Certificato No. 10000408125-MSC-ACCREDIA-ITA) si consulti il seguente indirizzo *web*: https://www.popso.it/cm/pages/ServeAttachment.php/L/IT/D/1%252Ff%252Fc%252FD.02490486df788c75795d/P/BLOB%3AID%3D1681/E/pdf?mode=download.

### *4.4 Discussione dei risultati*

Il processo di analisi tematica ha consentito in un primo momento di estrapolare i temi rilevanti ed emergenti oggetto di studio e di raggrupparli in *cluster*. In un secondo tempo, il processo di analisi narrativa ha consentito di ricostruire e organizzare separatamente la singolare esperienza *privacy* delle imprese. L'eccellente caso della Banca Popolare di Sondrio, unica impresa che non ha chiesto l'anonimato ai fini della ricerca, ha meritato un ulteriore approfondimento con una descrizione più dettagliata del singolo caso studio. In altri termini, i risultati della ricerca mostrano otto raggruppamenti tematici, sei differenti esperienze aziendali e un caso studio d'eccellenza. In linea generale, è possibile riscontrare un riguardevole impegno per la protezione dei dati da parte di tutte le imprese del campione della ricerca, differente in relazione al settore economico in cui operano e alle proprie esigenze aziendali. In particolar modo, l'impresa appartenente al settore delle telecomunicazioni e la Banca Popolare di Sondrio hanno abbracciato maggiormente l'impegno alla *privacy*, presumibilmente a causa della mole consistente di dati trattati che i settori economici pongono di loro natura. Il PIMS a cui fa riferimento il presente studio è stato adottato solamente da Banca Popolare di Sondrio, anche se, da quanto emerge dalla ricerca, l'impresa di telecomunicazioni ha in programma tale implementazione nei prossimi esercizi aziendali, mentre l'impresa operante nel settore *automotive* lo valuterà non appena avrà adottato la ISO/IEC 27001:2013. Quanto ai benefici, Banca Popolare di Sondrio ha ritenuto che il PIMS: (a) è direttamente integrabile a un sistema ISMS già esistente in azienda, (b) protegge la reputazione aziendale rassicurando i clienti e il *management* che i loro dati vengono gestiti in modo responsabile con le tecnologie più sofisticate senza violare la *privacy* degli interessati, (c)

fornisce una chiara visibilità dovuta alla corretta gestione dei dati e (d) la certificazione è sinonimo di conformità alla normativa europea. L'impresa appartenente al settore gomma-plastica utilizza il servizio BS10012:2017 in sinergia con ISO 27001 per garantire una corretta protezione dei dati, poiché non vi è ancora un metodo universalmente riconosciuto per garantire l'*accountability* al Reg. UE n. 2016/679. La *compliance* al GDPR viene garantita da tutte le imprese, talvolta anche con l'ausilio di altri *tool* di sistemi di gestione dei dati (GPDP), come nel caso dell'impresa agroalimentare, e addirittura mediante un sistema di gestione *privacy* autoprodotto con supporto di consulenti e collaborazioni con *cybersecurity team*, come nel caso interessante dell'impresa sanitaria. Il Sistema di Gestione della Sicurezza delle Informazioni (ISMS - ISO/IEC 27001) si conferma essere il più utilizzato; difatti, metà delle imprese del campione lo sta già adottando. I risultati della ricerca mostrano inoltre che metà delle imprese del campione non ha ottenuto alcuna certificazione né in materia di protezione dati personali né in materia di sicurezza delle informazioni, sebbene tutte le imprese abbiano conseguito altre certificazioni della serie ISO in ambiti differenti; in particolare, la quasi totalità delle imprese (5 su 6) è in possesso delle certificazioni ISO per i sistemi di gestione (a) della qualità, (b) per la salute e la sicurezza sul lavoro e (c) ambientale. Nell'ottica della responsabilità sociale globale d'impresa, tutte le imprese si impegnano anche in campi differenti alla protezione dei dati personali, accogliendo iniziative socialmente responsabili in disparati ambiti, che, nella totalità dei casi, vengono rendicontate (es. nel bilancio sociale). La responsabilità sociale delle imprese si articola in campo ambientale, lotta alla corruzione, risorse umane, rispetto dei diritti umani e pari opportunità, sicurezza sul lavoro, trasparenza, educazione e innovazione digitale, talvolta

con l'adozione di un codice etico. Nonostante ciò, in seguito alla piena attuazione del GDPR, si nota una maggiore considerazione dell'impegno in ambito *privacy* da parte delle imprese, dovuta non solo alla conformità al dettato normativo ma anche alle iniziative volte ad aumentare la consapevolezza di tale impegno (es. corsi di formazione). Sono state inoltre sondate le modalità di comunicazione della *privacy policy* (politica della *privacy*) che generalmente dipendono dal canale di raccolta dei dati e dalla tipologia di destinatari e avvengono ogni qualvolta vengono trattati dati personali. Quest'ultima rappresenta uno degli strumenti necessari per garantire ed applicare il principio base del Regolamento Europeo n. 679/2016: la protezione dei diritti e dei dati personali delle persone fisiche. Al postutto, si ribadisce che i vantaggi di *marketing* derivanti dall'esperienza *privacy* delle imprese sono frutto di una valutazione soggettiva dei DPO, i quali nella totalità dei casi hanno ritenuto che l'adozione di comportamenti socialmente responsabili in materia abbiano generato benefici dal lato impresa trascendenti il solo ambito del *marketing*, anche se non quantificati o misurati. Alla luce delle premesse teoriche iniziali e dei risultati ottenuti tramite la ricerca empirica, a mio giudizio, tutte le imprese del campione di riferimento possono essere definite socialmente responsabili, poiché, valutando e rispondendo alle aspettative economiche, non si sono limitate a soddisfare gli obblighi giuridici, ma sono andate oltre e hanno travalicato il minimo impegno previsto dalla legge, investendo ulteriormente in ambito *privacy* con l'obiettivo di creare valore e conseguire un vantaggio competitivo e in ultimo rendicontato in modo completo e trasparente il proprio impegno sociale ai pubblici di riferimento. Gli obiettivi della ricerca si considerano pertanto raggiunti e le domande di ricerca soddisfatte. La sottostante *Tabella 1* riepiloga in estrema sintesi i risultati della presente ricerca:

**Tabella 1. Risultati della ricerca**

| | Compliance GDPR | Implementazione PIMS ISO 27701 | Sistema di gestione dati (sicurezza e protezione) | Certificazioni sicurezza delle informazioni e protezione dati | Adozione altri standard normativi della serie ISO | Altre iniziative, comportamenti e pratiche socialmente responsabili | Modalità di comunicazione della privacy policy | Vantaggi di marketing ottenuti da impegno privacy |
|---|---|---|---|---|---|---|---|---|
| **Impresa nr. 1 (agroalimentare)** | Sì, altrimenti sanzioni. | No, ma ha definito serie di policy per la conformità GDPR. | Tool tramite la funzione GPDP. | Nessuna. | ISO22000 ISO14001 ISO50001 ISO45001 | Training e awareness in ambito privacy. Impegno sociale, ambientale, lotta alla corruzione, risorse umane, rispetto diritti umani. Progetto strutturato di sostenibilità. | Online. Report di sostenibilità. | Sì. Percorso di sostenibilità leva strategica. |
| **Impresa nr. 2 (gomma-plastica)** | Sì, ma non è esercizio statico. | No, poiché adotta PIMS del sistema BS10012 | ISMS in sinergia con BS10012 | ISO27001 BS10012 | ISO9001 ISO17025 ISO14001 ISO45001 | Adozione del codice etico. Principi di trasparenza, correttezza, lealtà. | No modalità standard. Digitale e dematerializzata. Dipendono dal tipo di raccolta dati e dai destinatari. | Competitività, etica d'impresa, consapevolezza interna importanza privacy. |
| **Impresa nr. 3 (automotive)** | Sì. | No, ma in valutazione. | ISMS (nel 2022). | Non ancora. | ISO9001 ISO14001 ISO45001 | In ambito human resources, sicurezza sul lavoro, ambientale. | Ogni qualvolta vengono trattati dati personali. Sito web, bilancio sociale. | Adozione sistema informativo di gestione della clientela (CRM) nel rispetto della normativa privacy. |
| **Impresa nr. 4 (telecomunicazioni)** | Sì, requisito indispensabile. | No, ma in programma. | ISMS --> PIMS | ISO27001 | ISO45001 ISO14001 | Approccio alla RSI si basa su: trasparenza, efficienza uso risorse, educazione e innovazione digitale, partecipazione e coinvolgimento. | Ogni volta che vengono trattati dati personali. Principalmente online. Sustainability report. | Sì, nell'ottica del marketing responsabile. Approccio alla RSI trasparente e integrato al core business. |
| **Impresa nr. 5 (sanitario)** | Sì, nell'ottica di aggiornamento. | No, in quanto di natura volontaria. | Sistema gestione privacy autoprodotto con supporto di consulenti esterni e cybersecurity team. | Nessuna. | ISO9001 ISO14001 ISO45001 | In ambito privacy istituiti corsi di formazione. Ambiente, sicurezza sul lavoro e anticorruzione. | Informativa privacy, canali online. Relazioni DPO e informativa annuale. | Sì. Evitare il danno di immagine per eventuali data breach è un vantaggio d'impresa. |
| **Impresa nr. 6 (credito)** | Sì. Provvedimenti organizzativi e operativi. | Sì, PIMS ex ISO 27701. | PIMS come estensione di ISMS. | ISO27001 ISO27701 | ISO9001 | Corsi privacy ai neo assunti. Aspetti sociali e attinenti alla gestione del personale, lotta alla corruzione, rispetto diritti umani. Adozione del Codice etico aziendale. | Dichiarazione consolidata di carattere non finanziario (DNF). Normali canali di comunicazioni delle prassi operative. Circolari aziendali, codice etico. | Sì. Benefici etica d'impresa a processi aziendali e sviluppo. |

### *4.5 Considerazioni finali*

L'attenzione mediatica al tema della *data protection* determina inevitabilmente una maggiore attenzione da parte degli *stakeholders* nel coinvolgere e nel rivolgersi a enti e imprese che investono risorse ed energie per attuare trattamenti di dati personali conformi al dettato normativo. Nella società digitalizzata e globalizzata di oggi, non abbiamo altra scelta che condividere le nostre informazioni personali. Tutto avviene *online*: dalle operazioni bancarie, alla spesa, alla prenotazione dei biglietti, agli appuntamenti e alla condivisione di foto. Poiché sempre più dati vengono raccolti ed elaborati, i consumatori, gli organismi di regolamentazione e i governi sono sempre più preoccupati per come vengono utilizzati e protetti da un uso improprio. Negli ultimi anni, non sono mancati scandali di alto profilo che coinvolgono aziende che raccolgono dati dei clienti senza autorizzazione o utilizzano informazioni in modo inappropriato o addirittura illegale. Oltre al modo in cui vengono utilizzati, è di fondamentale importanza il modo in cui le organizzazioni proteggono le nostre informazioni personali. I dati gestiti in modo improprio possono comportare la divulgazione di informazioni riservate e potenzialmente sensibili che portano a qualsiasi cosa, dal conto bancario di un cliente a violazioni della sicurezza nazionale. L'impatto aziendale sulle aziende colpite da un attacco informatico o coinvolte in uno scandalo di uso improprio dei dati può essere significativo. Dal risarcimento dei clienti all'indagine sull'incidente, i costi possono essere enormi. A lungo termine, la reputazione di un'azienda può essere gravemente danneggiata, così come il prezzo delle sue azioni. Per conquistare la fiducia dei consumatori e ottenere un vantaggio competitivo, le

aziende devono considerare la *data privacy* e la *data security* delle priorità assolute. La certificazione secondo uno *standard* internazionale riconosciuto è un valido strumento per proteggere la *privacy*. La pubblicazione di ISO/IEC 27701 (Sistema di gestione delle informazioni sulla *privacy*) nel 2019 come estensione di ISO/IEC 27001 (Sistema di gestione della sicurezza delle informazioni) fornisce un approccio di processo alle organizzazioni per aumentare naturalmente le loro pratiche di sicurezza delle informazioni esistenti per la protezione dei dati personali. A dimostrazione dell'importanza del nuovo *standard* normativo ISO/IEC 27701:2019 da utilizzare per i sistemi di gestione della protezione dei dati personali, vi sono i corsi di formazione organizzati da *Federprivacy*[351], indicati per *data protection officer*, funzionari *privacy*, responsabili dei sistemi informativi, responsabili dei sistemi di gestione aziendale, consulenti, *auditor*, e in generale come aggiornamento raccomandato per tutti i professionisti. Le organizzazioni che decidono di affrontare il processo volto ad ottenere una certificazione che attesta la conformità delle stesse alla norma internazionale ISO/IEC 27701:2019 forniscono adeguate garanzie della applicazione di una serie di misure a supporto dell'*accountability* prevista dal GDPR. Ogni procedura di certificazione comprende una

[351] FEDERPRIVACY è la principale associazione in Italia il cui principale scopo è radunare tutti i professionisti della *privacy* e della protezione dei dati, nonchè tutti gli altri addetti ai lavori che si occupano di tali tematiche, come i consulenti della *privacy*, *data protection officer* e *privacy officer*. Ma anche coloro che aspirano ad acquisire una qualificazione nell'ambito della *privacy*, possono beneficiare di tutti i vantaggi e le soluzioni riservate agli associati per il migliore svolgimento delle proprie attività in conformità della legislazione vigente. Per ulteriori informazioni in merito alla associazione si rimanda al sito *web* ufficiale: https://www.federprivacy.org/.

fase progettuale, preparatoria, redazionale ed applicativa. Segue poi una verifica di corretta applicazione del sistema gestionale, realizzata da un ente certificatore attraverso un ispettore abilitato. Peraltro, la creazione di dati è stata esponenziale negli ultimi anni e sta diventando il fulcro delle strategie di *business* digitale, il che contribuisce alla sua ubiquità. Nel 2020 la *International Data Corporation* ha pubblicato la sua previsione *Global DataSphere*[352] che mostra una crescita costante nella creazione e nel consumo di dati e ha affermato che la quantità di dati creati nei prossimi 3 anni sarà superiore ai dati creati negli ultimi 30 anni. Nello stesso rapporto si afferma anche che i dati della videosorveglianza e le iniziative sulla *privacy* e sulle normative continuano a intersecarsi. Trovare il giusto equilibrio tra sicurezza, protezione, personalizzazione, efficienza e diritti alla *privacy* sarà una delle grandi tensioni del prossimo decennio. Più che mai, c'è una crescente necessità per le organizzazioni di integrare la sicurezza e la protezione dei dati per raggiungere un equilibrio sostenibile tra il raggiungimento degli obiettivi aziendali e le politiche di responsabilità sociale.

[352] INTERNATIONAL DATA CORPORATION (IDC) è il principale fornitore globale di informazioni di mercato, servizi di consulenza ed eventi per i mercati della tecnologia dell'informazione, delle telecomunicazioni e della tecnologia di consumo. Le analisi e le comprensioni di IDC aiutano i professionisti IT, i dirigenti aziendali e la comunità degli investitori a prendere decisioni tecnologiche basate sui fatti e a raggiungere i propri obiettivi chiave aziendali. Il *Global DataSphere* quantifica e analizza la quantità di dati creati, acquisiti e replicati in un dato anno in tutto il mondo. Esamina anche la quantità di dati archiviati su vari supporti di archiviazione (HDD, SSD, NVM-NAND, NVM-altro, ottico e nastro) nel *Global StorageSphere*. Il rapporto è scaricabile *online* al seguente *link*: https://www.idc.com/getdoc.jsp?containerId=IDC_P38353.

## 5. Limiti della ricerca e traiettorie di ricerca futura

La ricerca empirica presentata poc'anzi è stata condotta in pieno periodo emergenziale da pandemia da *Covid-19* e questo rappresenta – a mio avviso – il più grande limite della ricerca. Pertanto, il disegno della ricerca ha subìto un considerevole ridimensionamento e una semplificazione rispetto al progetto originale elaborato nel periodo *pre-Covid*. In particolar modo a risentirne è stata la fase di raccolta dei dati e di conseguenza l'elaborazione degli stessi. Data l'impossibilità fisica di condurre la ricerca sul campo, si è optato per lo strumento d'indagine della intervista telefonica (semi-strutturata) a testimoni privilegiati (DPO). Data la modalità d'intervista a distanza, si è ritenuto indispensabile adattare la traccia al nuovo contesto, concependo una versione semplificata ma comunque idonea a soddisfare gli obiettivi della ricerca. Il campione ristretto è dovuto all'alto tasso di declinazioni e defezioni ricevute ai fini della ricerca in virtù della delicatezza del tema; pertanto, in fase di elaborazione dati, si è deciso di procedere solamente con l'analisi qualitativa. I limiti della presente ricerca aprono dunque le strade a svariate traiettorie di ricerca futura. Al di fuori dello stato di emergenza sanitaria, la stessa ricerca potrebbe essere condotta fisicamente sul campo, e in aggiunta anche dal punto di vista del consumatore e non solo dalla prospettiva dell'impresa. Aumentando considerevolmente il campione delle imprese oggetto di studio e cambiando lo strumento d'indagine, l'analisi dei dati potrebbe essere effettuata anche in maniera quantitativa. Inoltre, data l'impossibilità di misurare l'impegno *privacy* e il ritorno degli investimenti degli stessi, potrebbe essere creato un indicatore per quantificare i relativi vantaggi di *marketing*. I sistemi di gestione *privacy* autoprodotti schiudono scenari interessati e meritano approfondimento ulteriore.

## 6. Conclusioni e implicazioni per il management

La ricerca sin qui condotta ha mostrato l'adozione di pratiche socialmente responsabili in materia di *privacy* (con un particolare *focus* all'implementazione di un *Privacy Information Management System*) e, più in generale, anche in tutti gli altri ambiti direttamente riconducibili alla responsabilità sociale d'impresa (ad esempio iniziative in materia ambientale, sicurezza sui luoghi di lavoro, sistemi della gestione della qualità, pari opportunità, trasparenza e lotta alla corruzione). È stata inoltre assodata la modalità di comunicazione della *privacy policy* e delle altre pratiche di RSI, e verificata l'adozione (con conseguente ottenimento della certificazione) degli *standard* normativi della serie ISO. In aggiunta, sono stati rielaborati i vantaggi di *marketing* ottenuti dalle imprese mediante l'impegno alla protezione dei dati, secondo il punto di vista dei DPO che hanno partecipato alla indagine. Questo lavoro intende in conclusione fornire una guida d'incoraggiamento per le organizzazioni che desiderano implementare un PIMS certificato ISO/IEC 27701:2019 per supportare la conformità al GDPR. Appare chiaro che alla base del presente lavoro vi sia la gestione responsabile (v. cap. 1), un imperativo su cui fondare la gestione d'impresa, che impone di rivedere le proprie pratiche e i rapporti con gli innumerevoli *stakeholder*. Si tratta di un concetto sul quale le imprese sono sempre più chiamate a riporre la loro attenzione e a sviluppare una propria politica in merito. Presupposto di fondo della RSI è il principio di *accountability* (responsabilizzazione), ovvero il dovere di rendicontare in modo completo e trasparente il proprio impegno sociale ai pubblici di riferimento (v. cap. 3 par. 4). La nuova normativa europea in materia di protezione dati

(GDPR) impone un sistema basato sulla responsabilità e impostato su una serie di obblighi in capo al titolare del trattamento, consistenti in obblighi generali (art. 24) e obblighi concernenti la sicurezza di tipo preventivo e successivo (artt. 32 ss.), nonché adempimenti di valutazione d'impatto e consultazione preventiva (artt. 35 ss.), cui si aggiungono le disposizioni di *privacy by design* e *privacy by default*, intesi come strumenti di protezione *ex ante* e *life-long* dei dati. Il nuovo approccio al rischio (*risk-oriented approach*) appare tutto incentrato nella sfera del titolare, nelle declinazioni di una maggiore proceduralizzazione degli obblighi dello stesso e del principio di *accountability*, che si traduce in *compliance* dei trattamenti (v. cap. 3 par. 3). Non per tutte le realtà aziendali è facile assicurare la *compliance* al GDPR perché la normativa europea non indica con precisione cosa fare in concreto per rendersi *compliant*, ma spiega quali procedure adottare per non correre rischi in materia di *data protection*. Il GDPR, infatti, non fornisce un elenco di adempimenti cui sottostare che garantiscano la piena *compliance*, ma dà delle indicazioni generiche lasciando piena libertà al titolare del trattamento, che dovrà semplicemente provare di avere adottato tutte le misure adeguate a tutelare la *privacy* in ossequio al principio di responsabilizzazione (v. cap. 3 par. 4). È necessario, dunque, da parte delle imprese, individuare sistemi di valutazione di aderenza al modello e dotarsi di organizzazioni competenti, processi strutturati e competenze professionali idonee al compito. La ISO 27701:2019 di recente introduzione arriva dopo l'introduzione in Europa del GDPR, il quale ha prodotto un duplice effetto, rappresentando un'innovazione e un'armonizzazione rispetto alle normative esistenti sulla

*privacy* dei dati, che riflettono le realtà del mondo digitale in cui viviamo. Sviluppato dal comitato tecnico ISO SC27 con *input* da 25 organismi esterni, compreso il Comitato europeo per la protezione dei dati (EDPB), è uno degli *standard* su base volontaria più attesi in merito alla sicurezza delle informazioni e gestione della *privacy*. La normativa specifica i requisiti per progettare, creare, implementare, gestire, monitorare, revisionare, mantenere e migliorare in modo continuo un *Privacy Information Management System* (v. cap. 4). Le organizzazioni con il desiderio di affrontare le sfide della conformità in materia di sicurezza delle informazioni e protezione dei dati possono trarre vantaggio dall'implementazione del nuovo *standard* normativo. Lo *standard* illustra un *set* completo di controlli operativi che può essere adattato alle diverse normative internazionali, incluso il GDPR. Dopo aver eseguito il *mapping*, i controlli operativi del PIMS vengono implementati da professionisti della *privacy* e controllati da revisori interni o da terze parti, con conseguente certificazione e prova della conformità. Implementare un PIMS conforme alla ISO/IEC 27701 consente alle organizzazioni di soddisfare i requisiti del GDPR e di altre regolamentazioni internazionali e nazionali in materia di protezione dei dati e dimostra che sono state predisposte misure tecniche e organizzative appropriate (art. 32) per proteggere i dati personali che vengono trattati, proteggendo i diritti degli interessati, in linea con il principio di *accountability* (art. 5). Nella ISO 27701 si trova, per fare un esempio, l'attenzione sulla gestione delle risorse umane in fase di assunzione, in fase di passaggio di responsabilità interna e anche in fase di dimissione o uscita dall'azienda – oppure – la gestione degli *asset* presenti in azienda, o il controllo e le politiche relative agli accessi, e

ancora i controlli sulla crittografia, o la gestione della sicurezza di aree fisiche o logiche o ancora la sicurezza delle connessioni. La ISO/IEC 27701 rappresenta quindi un importante strumento per i vari *stakeholder* coinvolti nella protezione dei dati personali, come ad esempio per le organizzazioni che hanno uno schema dettagliato di requisiti e controlli da implementare per dimostrare la conformità alla legislazione vigente; per i DPO, che hanno uno strumento dettagliato per adempiere a quanto richiesto dall'art. 39 par. 1 punti (a) e (b); e per gli organi ispettivi che hanno a disposizione una *checklist* dettagliata rispetto alla quale poter impostare i controlli di merito. Nonostante il crescente regime normativo sulla *privacy* a livello globale, non esiste un modo universalmente riconosciuto per ottenere la totale conformità (*compliance*) o dimostrare che un'organizzazione può essere considerata *compliant* per il proprio approccio alla *privacy*. Alla luce di questi razionali, la normativa ISO/IEC 27701 si poneva come candidato ideale per realizzare uno schema di certificazione dei trattamenti di dati personali come previsto dal GDPR al Capo IV sezione 5 artt. 42 e 43 – Codici di condotta e certificazioni, oltre che in diversi *considerando* (98,99,100,167,168). Per un'organizzazione che è già certificata ISO 27001, l'implementazione della ISO 27701 può essere un utile e conveniente mezzo per dimostrare la propria attitudine *privacy-friendly*. Per un'organizzazione che invece non è dotata di un Sistema di Gestione per la Protezione delle Informazioni, la ISO 27701 non è la risposta all'art. 43 e non può essere considerata certificazione al GDPR. Per poter rispondere positivamente alle richieste degli artt. 42 e 43 del Regolamento europeo 2016/679, la certificazione dovrà essere specifica e fornire un'assicurazione diretta tale per

cui vi sia una rispondenza diretta (v. cap. 4 par. 7) fra il trattamento/processo e i requisiti applicabili con una trasposizione puntuale di articoli e *considerando*. Il meccanismo di certificazione *ex* GDPR è ancora in corso di definizione sia a livello italiano che a livello europeo. L'approccio di un'impresa alla *privacy* dipende dunque dalle prospettive morali dei *leader* e la prospettiva etica del *top management* determina se una impresa sarà proattiva nell'impostazione e supporto di tali politiche. L'etica aziendale (v. cap. 1 par. 5), poiché è rivolta a conciliare gli obiettivi economici e le responsabilità sociali, può essere considerata come un modello comportamentale di sintesi funzionale allo sviluppo dell'impresa e alle finalità dell'imprenditore nel lungo termine. Un avanzamento sostanziale si verifica quando l'etica viene considerata come un'opportunità e non come un vincolo nel governo d'impresa. In quest'ottica i princìpi etici non devono essere considerati contrapposti ai princìpi economici di efficienza ed efficacia, ma come un sistema complesso di valori capace di conciliare, in modo più equo e durevole, interessi interni ed esterni all'impresa e che consentano lo sviluppo di una gestione aziendale più corretta e il miglioramento dei risultati d'impresa. L'applicazione dell'etica alle decisioni di *marketing* rappresenta un'esigenza per le imprese, non soltanto per una motivazione reputazionale, ma per rispondere al principio di soddisfazione degli *stakeholder* e, in particolare, dei clienti, in considerazione della differente posizione di forza che le imprese, soprattutto quelle di grandi dimensioni, possono esercitare nei loro confronti. La vera sfida del *marketing* socialmente responsabile (v. cap. 1 par. 4) è abbracciare l'area della sostenibilità: in questo caso il beneficio di breve e lungo periodo della collettività si affianca e non si sostituisce al

vantaggio del consumatore, per garantire la sostenibilità economica e sociale dell'impresa. L'impresa che voglia avviarsi verso un percorso di sostenibilità deve sostanzialmente ampliare lo spettro delle proprie responsabilità. Un approccio sostenibile, ossia capace di far sopravvivere l'impresa nel lungo periodo, impone ben altre attenzioni che il mero perseguimento della creazione di valore per gli azionisti. Le imprese possono scegliere di concentrarsi sulla conformità al minimo costo possibile, giocando al passo con le autorità di regolamentazione e offrendo al contempo un'esperienza mediocre per i clienti, oppure possono sfruttare la conformità per stimolare la cultura aziendale e identificare la *privacy* come uno dei valori fondamentali dell'organizzazione. Difatti, l'architettura giuridica di riferimento in merito ai meccanismi di responsabilità prevede due livelli, dei quali il primo è costituito da un obbligo di base vincolante per tutti i titolari del trattamento, consistente nell'attuazione di misure e procedure e nella conservazione delle relative prove, mentre il secondo livello include sistemi di responsabilità di natura volontaria eccedenti le norme di legge minima, in relazione ai principi fondamentali di protezione dei dati (tali da fornire garanzie più elevate di quelle prescritte dalla normativa vigente) e/o intermedi modalità di attuazione di garanzia dell'efficacia delle misure (norme di attuazione) e consistente nell'obbligo di conformarsi. Un'impresa che adotti un comportamento socialmente responsabile, valutando e rispondendo alle aspettative economiche, ambientali e sociali di tutti gli *stakeholders* travalicando il minimo impregno previsto dalla legge, coglie l'obiettivo di creare valore e conseguire un vantaggio competitivo. Al contrario, comportamenti poco etici o la mancanza di strategie di sostenibilità e

responsabilità sociale delle imprese possono danneggiare la reputazione di un'azienda e renderla meno attraente per gli azionisti, con conseguente riduzione dei profitti. In altri termini, qualora le imprese decidessero spontaneamente di aderire ad altri livelli di RSI (v. Piramide di Carroll cap. 3 par. 2), non si limiteranno a soddisfare gli obblighi giuridici, ma potranno andare oltre investendo ulteriormente nel capitale umano e nei rapporti con gli *stakeholders*. La inevitabile conseguenza è il mutamento del ruolo e della concezione dell'impresa stessa: si assiste al passaggio dalla logica del profitto e dello sviluppo a discapito della società civile alla visione eticamente orientata dell'attività di impresa (v. cap. 1 par. 5). Per tutto ciò, la protezione dei dati in sé rappresenta una nuova forma di responsabilità sociale d'impresa. Certo è che in seguito all'entrata in vigore del GDPR, le imprese hanno cessato di considerare la protezione dei dati come un semplice obbligo di conformità legale, vissuto e interpretato in ambito imprenditoriale come un mero obbligo burocratico che rallenta o rende più macchinoso il raggiungimento degli obiettivi d'impresa. Nello scenario che si sta configurando, sempre più incentrato sui dati (v. cap. 2 par. 8), le imprese considerano la *privacy* come risorsa che aiuta a perseguire responsabilmente i propri obiettivi economici e una solida politica aziendale può consentire l'elaborazione dei dati in modo responsabile e sostenibile e promuovendo appieno il loro potenziale (v. cap. 3 par. 2). Oggi, garantire la *compliance* all'interno della propria azienda è diventato un sinonimo di qualità dell'intera organizzazione: dai prodotti, ai processi, fino ai sistemi. In altri termini, garantire l'*accountability* rappresenta un valore aggiunto che permette di distinguersi dalla concorrenza e di guadagnare una posizione di

vantaggio nel proprio settore, specialmente nel caso in cui il cui *core business* dell'azienda si basi sulla raccolta e l'elaborazione dei dati forniti dai clienti.

## 7. Appendice della ricerca

Trascrizione delle interviste ai *Data Protection Officer* delle imprese in qualità di testimoni privilegiati.

Impresa nr. 1 settore agroalimentare

**D**: Il 25 maggio 2018 – a seguito della piena attuazione del Regolamento europeo 2016/679 – è iniziata l'era del *General Data Protection Regulation*. L'impresa si presenta conforme a tutte le disposizioni coercitive in materia di protezione dei dati personali?

**R**: Sì, altrimenti l'impresa incorrerebbe nelle sanzioni penali e amministrative previste in caso di violazione o mancato adeguamento. Al contempo, abbiamo definito una serie di *policy* per la gestione dei requisiti del GDPR e anche implementato un *tool* che permette di gestire e tracciare le principali attività richieste dallo stesso GDPR, al fine di essere in grado di dimostrare efficacemente la conformità.

**D**: A seguito della piena attuazione del GDPR, l'impresa ha adottato su base volontaria il nuovo *standard* normativo ISO/IEC 27701:2019 per l'implementazione del *Privacy Information Management System*?

**R**: No, l'impresa non si è dotata di questo *standard* normativo ma rispetta scrupolosamente quanto previsto dal GDPR.

**D**: L'impresa è dotata di un altro sistema per la gestione e sicurezza dei dati e delle informazioni? Ad esempio, la ISO 27001 o la BS 10012.

**R**: No, l'impresa non si è dotata nello specifico di questi sistemi per la protezione dei dati. Tramite la funzione *Group Privacy and Data Protection*, la società ha gestito il progetto di adeguamento al nuovo Regolamento Europeo in materia di protezione dei dati personali e in questo rispetto è stato nominato il *Data Protection Officer* ed è stato inoltre definito un modello organizzativo in materia di protezione dei dati personali, identificando ruoli e responsabilità.

**D**: L'impresa ha ottenuto dalle autorità preposte certificazioni e accreditamenti inerenti alla protezione dei dati personali?

**R**: In materia di protezione dei dati no, o perlomeno, non ancora.

**D**: L'impresa ha adottato *standard* normativi della serie ISO e ottenuto le relative certificazioni anche in ambiti differenti alla protezione dei dati?

**R**: Sì, il gruppo ha mantenuto la *compliance* agli *standard* internazionali di sicurezza alimentare ottenendo la ISO22000 e ha definito un programma di certificazioni per migliorare le *performance* nei prossimi anni. Quanto alle certificazioni ambientali, il gruppo ha ottenuto la

ISO14001 e la ISO50001 e in ultimo la certificazione ISO45001 in ambito salute e sicurezza.

**D**: L'impresa ha adottato altri comportamenti e pratiche socialmente responsabili in altri ambiti oltre che in materia di *privacy*?

**R**: Sì, certo, tutte le politiche sono menzionate nei *report* di sostenibilità. Il gruppo si impegna costantemente in ambito sociale, ambientale, lotta alla corruzione, risorse umane, rispetto dei diritti umani. Tornando alla protezione dei dati, nell'ambito delle attività progettuali, sono state eseguite numerose attività di *training* e *awareness*.

**D**: Come viene comunicata la *privacy policy* agli *stakeholder* dell'impresa?

**R**: Generalmente *online*. La nostra *privacy policy* è riportata nelle relazioni di sostenibilità. Inoltre, nell'ambito delle sue attività, il gruppo ha ritenuto necessario definire un progetto strutturato dedicato alla sostenibilità, con l'obiettivo di diffondere internamente la cultura della responsabilità d'impresa, realizzare progetti a supporto delle persone e condividere con gli *stakeholder* i risultati ottenuti, il tutto sempre rendicontato nella relazione di sostenibilità.

**D**: L'impresa ha ottenuto vantaggi di *marketing* derivanti da comportamenti socialmente responsabili in materia di *privacy*?

**R**: Difficile darne una quantificazione ma, ciononostante, sicuramente sì. Il percorso di sostenibilità del gruppo è stato avviato ufficialmente nel 2011, con l'ambizione di

rendere la sostenibilità una delle leve strategiche per la crescita e per la definizione delle politiche aziendali.

Impresa nr. 2 settore gomma–plastica

**D**: L'impresa si presenta conforme a tutte le disposizioni coercitive in materia di protezione dei dati personali previste dal GDPR?

**R**: Sì, fermo restando che la *compliance* al GDPR non è un esercizio statico.

**D**: A seguito della piena attuazione del GDPR, l'impresa ha adottato su base volontaria la nuova normativa ISO/IEC 27701 per l'implementazione del *Privacy Information Management System*?

**R**: No, non è stata adottata, ma è stata implementata la normativa ISO 27001 per la sicurezza delle informazioni in combinazione sinergica con il servizio BS 10012 per le peculiarità della protezione dei dati in linea con la normativa europea, anche se non in tutti i Paesi in cui l'impresa opera.

**D**: L'impresa ha adottato altri *standard* normativi della serie ISO ottenendo le relative certificazioni in ambiti differenti alla protezione dei dati?

**R**: Riguardo alla protezione dei dati personali, Le ricordo che il meccanismo di richiesta e attribuzione delle certificazioni è ancora in corso di definizione sia a livello italiano che europeo, secondo quanto dispone il GDPR agli artt. 42 e seguenti. Siamo comunque per ora certificati ISO27001 e BS10012. Oltre a ciò, l'impresa svolge

un'intensa attività nel campo dei sistemi di gestione, avvalendosi di questi strumenti per migliorare la qualità, l'efficacia e l'efficienza dei propri processi, nonché al fine di perseguire un'ulteriore riduzione degli impatti sulla salute dei dipendenti, sulle condizioni di sicurezza del lavoro e sull'ambiente esterno. Infatti, sono state ottenute le certificazioni di qualità ISO 9001 e ISO/IEC 17025, la certificazione ISO 14001 per l'ambiente e infine la ISO 45001 per il sistema salute e sicurezza.

**D**: L'impresa ha adottato altri comportamenti e pratiche socialmente responsabili in altri ambiti oltre che in materia di *privacy*?

**R**: Sì, si è adottato un Codice etico, dove sono rappresentati i principi generali di trasparenza, correttezza e lealtà cui si ispira lo svolgimento e la conduzione degli affari. Il codice indica gli obiettivi e i valori informatori dell'attività d'impresa, con riferimento ai principali *stakeholders* con i quali ci si trova quotidianamente a interagire: azionisti, mercato finanziario, clienti, comunità personale.

**D**: Come viene comunicata la *privacy policy* agli *stakeholder* dell'impresa?

**R**: Le modalità di comunicazione delle *privacy policy* dipendono dal canale di raccolta dei dati personali e dalla tipologia di destinatari, non vi è tuttavia una modalità *standard* di comunicazione. La società privilegia tendenzialmente modalità di comunicazione di tipo digitale o comunque dematerializzate.

**D**: L'impresa ha ottenuto vantaggi di *marketing* derivanti da comportamenti socialmente responsabili in materia di *privacy*?

**R**: I vantaggi derivanti da comportamenti socialmente responsabili in materia di *privacy* sono vari e trascendono il solo ambito del *marketing*. In generale, tali comportamenti hanno avuto e continuano ad avere ricadute positive sia in termini di competitività della società, sia in termini di etica d'impresa e consapevolezza interna dell'importanza della *privacy*.

Impresa nr. 3 settore automobilistico

**D**: Il 25 maggio 2018 – a seguito della piena attuazione del Regolamento europeo 2016/679 – è iniziata l'era del *General Data Protection Regulation*. L'impresa si presenta conforme a tutte le disposizioni coercitive in materia di protezione dei dati personali?

**R**: Sì, certamente.

**D**: A seguito della piena attuazione del GDPR, l'impresa ha adottato su base volontaria il nuovo *standard* normativo ISO/IEC 27701:2019 per l'implementazione del *Privacy Information Management System*?

**R**: No, in quanto appunto di natura volontaria. L'eventuale avvio di un processo di adozione e certificazione ISO/IEC 27701 verrà valutato a seguito dell'ottenimento della certificazione ISO 27001.

**D**: L'impresa è dotata di un sistema per la gestione e sicurezza dei dati e delle informazioni?

**R**: No, ma è prevista la certificazione ISO/IEC 27001 entro il 2022.

**D**: L'impresa ha ottenuto dalle autorità preposte certificazioni *privacy*?

**R**: No, nessuna.

**D**: L'impresa ha adottato altri *standard* normativi della serie ISO con conseguenti certificazioni in ambiti differenti alla protezione dei dati?

**R**: Il gruppo vanta sistemi di gestione dell'ambiente, della qualità e della sicurezza del lavoro di eccellenza in tutti i suoi siti produttivi e di conseguenza è certificato ISO 9001 per i sistemi di gestione della qualità, ISO 14001 per i sistemi di gestione ambientale e ISO 45001 per i sistemi di gestione per la salute e la sicurezza sul lavoro.

**D**: L'impresa ha adottato altri comportamenti e pratiche socialmente responsabili in altri ambiti differenti il contesto *privacy*?

**R**: Decisamente. In ambito *human resources*, tramite una corretta gestione delle diversità e un'offerta di pari opportunità a entrambi i sessi. Per quanto riguarda la sicurezza sul lavoro, il gruppo ha intrapreso azioni concrete finalizzate a consentire una evoluzione continua per un lavoro più sicuro che parte dalla valutazione degli aspetti relativi alla sicurezza dell'ambiente di lavoro ed ai relativi strumenti, fin dalle fasi di definizione delle nuove attività, o nella revisione di quelle esistenti e comportamenti più sicuri attraverso la formazione, informazione e sensibilizzazione di tutti i lavoratori, per consentire loro di svolgere i propri compiti in sicurezza e di assumere la responsabilità in materia di salute e sicurezza sul lavoro. In campo ambientale, il gruppo ha definito una specifica struttura organizzativa preposta al perseguimento degli

obiettivi di sostenibilità ambientale dei propri siti produttivi.

**D**: Come viene comunicata la *privacy policy* agli *stakeholder* dell'impresa?

**R**: La società comunica la propria *privacy policy* attraverso il proprio sito *web*, il bilancio sociale e ogni qual volta vengano trattati dati personali.

**D**: L'impresa ha ottenuto vantaggi di *marketing* derivanti da comportamenti socialmente responsabili in materia di *privacy*?

**R**: Il *business* aziendale relativo al settore *automotive* non rientra tra quelli ad elevata presenza e gestione di dati personali, come ad esempio gli istituti di credito e le compagnie telefoniche. Conseguentemente, la società, che comunque tratta dati personali, si è dotata di un apposito sistema informativo di gestione della clientela e del relativo *marketing*, il cosiddetto *Customer relationship management*, utilizzato nel rispetto della normativa *privacy*. Inoltre, come indicato nell'ultimo *report* di *corporate social responsibility* pubblicato, non si registrano, nel corso dell'ultimo anno 2020, casi di reclami relativi a violazioni della *privacy* o perdita dei dati dei clienti. E per di più non risultano sanzioni riferite alla non conformità a leggi e regolamenti, incluse leggi e regolamenti di natura ambientale, attività di *marketing*, pubblicità, promozione, sponsorizzazione, fornitura ed utilizzo dei prodotti.

Impresa nr. 4 settore telecomunicazioni

**D**: Il 25 maggio 2018 – a seguito della piena attuazione del Regolamento europeo 2016/679 – è iniziata l'era del *General Data Protection Regulation*. L'impresa si presenta conforme a tutte le disposizioni coercitive in materia di protezione dei dati personali?

**R**: Sì, ci presentiamo conformi alle disposizioni. La corretta gestione dei dati aziendali e dei clienti (soprattutto personali, ma non solo) da parte dell'azienda è un requisito indispensabile per la sua credibilità sul mercato. L'azienda adotta quindi stringenti misure di garanzia e supporta numerose attività in questo ambito. Il tema della *privacy* e della sicurezza dei dati è molto sensibile per un'azienda come la nostra, che custodisce un'enorme quantità di informazioni relative ai clienti e alle loro abitudini e preferenze. La principale sfida in questo senso è proprio riuscire a coniugare la complessità richiesta dagli obblighi normativi con l'estrema semplicità nell'esperienza degli utenti e nella fruizione dei servizi. Il tutto in un contesto molto dinamico caratterizzato da una continua evoluzione del *business* e delle tecnologie associate. La politica aziendale sul tema della *privacy* e sicurezza dei dati mira innanzitutto a garantire la conformità normativa, con riferimento al contesto legislativo sia nazionale che comunitario, tenendo conto dell'introduzione del nuovo GDPR e anche dell'introduzione della nuova normativa sui temi della *cybersecurity*.

**D**: A seguito della piena attuazione del GDPR, l'impresa ha adottato su base volontaria il nuovo *standard* normativo ISO/IEC 27701:2019 per l'implementazione del *Privacy Information Management System*?

**R**: Non ancora, dato che l'adozione della nuova ISO per l'implementazione di un PIMS rientra nei punti programmatici dei prossimi esercizi aziendali.

**D**: Oltre la *compliance* normativa al GDPR, l'impresa è dotata di un altro sistema per la gestione e sicurezza dei dati e delle informazioni o ha in programma l'adozione di un altro sistema di protezione?

**R**: Sì, la ISO/IEC 27001 per la sicurezza delle informazioni già da diversi anni. Gli impatti relativi alla gestione dei dati dei clienti ricadono sotto la diretta responsabilità dell'azienda per quanto riguarda le informazioni archiviate ma possono anche derivare dalle relazioni di *business* che l'azienda intrattiene con soggetti terzi, che gestiscono parte dei processi commerciali e di assistenza e che, di conseguenza, hanno necessità di operare sui dati dei clienti in piena legittimità normativa tramite la loro nomina a responsabili del trattamento. Grazie anche ai processi di armonizzazione avvenuti negli anni precedenti, l'azienda adotta oggi un sistema di *governance*, *risk management* e *compliance* che consente di tenere sotto controllo l'intera filiera del trattamento dei dati, valutando in maniera analitica il livello di conformità di ciascun sistema coinvolto. Periodicamente, sono effettuate delle specifiche attività di monitoraggio con tutti i responsabili aziendali nell'ambito della tenuta del registro dei trattamenti nonché attività di verifica tramite un sistema di autovalutazione di tutti i fornitori nominati responsabili del trattamento.

**D**: L'impresa ha ottenuto dalle autorità preposte certificazioni e accreditamenti inerenti alla sicurezza o protezione dei dati?

**R**: La DNV, uno dei principali enti di certificazione a livello mondiale, ha riconosciuto all'azienda il mantenimento delle certificazioni relative ai temi di sicurezza delle informazioni ISO/IEC 27001.

**D**: L'impresa ha adottato altri *standard* normativi della serie ISO ottenendo le relative certificazioni in ambiti differenti alla protezione dei dati?

**R**: L'azienda conferma il proprio impegno nell'integrare la sostenibilità con la gestione del *business*, per contribuire alla realizzazione degli obiettivi dell'Agenda 2030. In ambiti diversi rispetto alla protezione dati, l'azienda ha raggiunto certificazioni relative ai temi di Salute e Sicurezza sul Lavoro (ISO 45001), Ambiente (ISO 14001), Responsabilità sociale (SA 8000), Qualità (ISO 9001). Questo risultato è stato conseguito nel contesto straordinario determinato dall'emergenza *coronavirus*, che ha richiesto l'utilizzo di nuovi modelli nello svolgimento delle verifiche, sia in presenza sia da remoto, recependo ed implementando tutte le misure di prevenzione in linea con i provvedimenti disposti dalle autorità di governo e sanitarie.

**D**: L'impresa ha adottato altri comportamenti e pratiche socialmente responsabili in materia di *privacy* non menzionate finora? L'impresa si impegna anche in altri ambiti?

**R**: Fin dalla nostra nascita abbiamo rendicontato volontariamente i nostri impatti sociali e ambientali. L'approccio dell'azienda alla responsabilità d'impresa si basa sostanzialmente su quattro punti alla base del rapporto dell'azienda con i propri *stakeholder* e delle attività di

responsabilità sociale e ambientale che sono: 1. trasparenza e approccio a 360°; 2. efficienza nell'uso delle risorse; 3. educazione e innovazione digitale; 4. partecipazione e coinvolgimento nella comunità. L'azienda esiste per eliminare qualsiasi distanza tra le persone, per questo motivo pensiamo che ci sia un solo modo per garantire un futuro sostenibile, responsabile e inclusivo per tutti: disegnarlo insieme, appunto.

**D**: Come vengono comunicati la *privacy policy* e l'impegno alla *privacy* agli *stakeholder* dell'impresa?

**R**: Principalmente *online* e più in generale ogni volta vengono trattati dati personali. Il nostro *Sustainability Report* 2020 – per esempio – racconta ciò che abbiamo fatto in un anno particolare e difficile. Un anno nel quale, tra l'altro, abbiamo rilanciato i nostri obiettivi di sostenibilità con orizzonte al 2030, insieme ai nostri *manager*, ai nostri giovani e ai nostri principali *stakeholder*. La *privacy* per noi è parte integrante della *responsibility*, una delle quattro aree del nostro modello di sostenibilità. È iniziata una nuova era per la responsabilità: rispettare le regole non basta, dobbiamo immaginarne di nuove per rispondere alle sfide della rivoluzione digitale. Noi ci impegniamo quotidianamente per tutelare la sicurezza in rete cercando di raggiungere *standard* sempre più elevati. Sicurezza per noi significa proteggere i dati sensibili e la *privacy* di tutti gli utenti con cui interagiamo, ma soprattutto tutelare le fasce più vulnerabili dalle potenziali minacce *online*.

**D**: Ritiene che l'impresa abbia ottenuto vantaggi di *marketing* derivanti da comportamenti socialmente responsabili in materia di *privacy*?

**R**: Sicuramente sì, l'azienda adotta pratiche commerciali corrette ed improntate al principio della trasparenza, della chiarezza, della semplicità e della correttezza verso i clienti nell'ottica di un *marketing* responsabile. L'azienda crede in un approccio alla responsabilità sociale d'impresa trasparente ed integrato con il *core business*. Rendicontiamo regolarmente sui nostri impatti e le nostre scelte, in base agli interessi dei nostri *stakeholder*, e sosteniamo attivamente il valore della trasparenza, anche nella società italiana. Responsabilità significa anche verificare la correttezza di ogni nostra attività, ad iniziare da quelle legate al *business*. L'eventualità di una significativa perdita di dati comporterebbe per l'azienda dei rischi rilevanti sotto il profilo reputazionale, economico e operativo. Con questa consapevolezza l'azienda attua, quindi, tutte le misure necessarie a presidiare accuratamente la sicurezza dei dati, delle informazioni così come il rispetto della *privacy* e delle recenti normative in tema di *cybersecurity*, nell'interesse dei clienti e dell'azienda stessa. Inoltre, l'azienda si prefigge di prevenire eventuali perdite o danneggiamenti dei dati gestiti, limitare i danni e ripristinare la normale operatività aziendale nel più breve tempo possibile, nel caso di eventuali incidenti.

Impresa nr. 5 settore sanitario

**D**: L'impresa si presenta conforme a tutte le disposizioni coercitive in materia di protezione dei dati personali previste dal GDPR?

**R**: Sì, ci presentiamo conformi a tutte le disposizioni previste dal GDPR, nell'ottica comunque di un continuo aggiornamento.

**D**: A seguito della piena attuazione del GDPR, l'impresa ha adottato su base volontaria il nuovo *standard* normativo ISO/IEC 27701:2019 per l'implementazione del *Privacy Information Management System*?

**R**: No, poiché basato sulla volontarietà.

**D**: Oltre la *compliance* normativa al GDPR, l'impresa è dotata di un altro sistema per la gestione e sicurezza dei dati e delle informazioni o ha in programma l'adozione di un altro sistema di protezione?

**R**: Sì, l'azienda si è dotata di un sistema di gestione *privacy* autoprodotto con supporto di consulenti e collaborazioni con *cybersecurity team*.

**D**: L'impresa ha ottenuto dalle autorità preposte certificazioni inerenti alla protezione dei dati personali?

**R**: No, e non sono ancora disponibili certificazioni secondo il GDPR.

**D**: L'impresa ha adottato altri *standard* normativi della serie ISO ottenendo le relative certificazioni in ambiti differenti alla protezione dei dati?

**R**: Sì, ISO 9001, ISO 14001 e ISO 45001.

**D**: L'impresa ha adottato altri comportamenti e pratiche socialmente responsabili in materia di *privacy* non menzionate finora? L'impresa si impegna anche in altri ambiti?

**R**: Sì, in particolare in ambiente, sicurezza sul lavoro e anticorruzione.

**D**: Come vengono comunicati la *privacy policy* e l'impegno alla *privacy* agli *stakeholder* dell'impresa?

**R**: Principalmente tramite l'informativa *privacy*, i canali *online* e le relazioni del DPO. Sono stati istituiti dei corsi di formazione in presenza, con l'aiuto di infografiche e *videoclip*, e dei corsi *online*, avvalendosi di *Intranet*. C'è poi un'informativa annuale.

**D**: Ritiene che l'impresa abbia ottenuto vantaggi di *marketing* derivanti da comportamenti socialmente responsabili in materia di *privacy*?

**R**: Non quantificabili in quanto non misurati, ma – a mio giudizio – sicuramente sì. Ritengo che evitare il danno d'immagine per eventuali *data breach* costituisca già un obiettivo e dunque un vantaggio d'impresa.

Intervista nr. 6 a Banca Popolare di Sondrio

**D**: Il 25 maggio 2018 è iniziata l'era del *General Data Protection Regulation*. La Banca si presenta conforme a tutte le disposizioni coercitive in materia di protezione dei dati personali?

**R**: Sì, e a sostegno e presidio di tale tema Banca Popolare di Sondrio ha adottato dei provvedimenti organizzativi, collocando internamente il ruolo di DPO all'interno della Funzione di Conformità creando un'unità organizzativa apposita di Presidio Operativo (il cosiddetto Presidio Operativo di protezione dei dati personali) all'interno dell'Ufficio Gestione e Protezione dei dati. Sono stati adottati inoltre provvedimenti operativi con l'emissione nel 2018 da parte del Consiglio di Amministrazione dell'articolato "Regolamento in materia di Protezione dei Dati Personali" correlato di specifici modelli operativi, organizzativi e di controllo a copertura dei vari aspetti della tematica, come contratti e nomine a responsabile esterno, diritti degli interessati, registro dei trattamenti… e via dicendo.

**D**: A seguito della piena attuazione del GDPR, l'impresa ha adottato su base volontaria il nuovo *standard* normativo ISO/IEC 27701:2019 per l'implementazione del *Privacy Information Management System*?

**R**: Sì. La Banca dispone di un articolato *framework* integrato di sicurezza e gestione dei rischi ICT, fortemente basato sugli *standard* ISO. Ormai da diversi anni la Banca, ed in particolare il *framework* integrato di gestione dei rischi ICT adottato dai sistemi informativi, sono certificati ISO 27001. In particolare, tale *standard* ISO27701 è stato

certificato, a seguito di accertamenti condotti dall'ente di certificazione DNV (*Det Norske Veritas*) per l'ambito dei sistemi informativi ufficialmente nel dicembre 2020.

**D**: Potrebbe raccontare l'esperienza di implementazione del PIMS di Banca Popolare di Sondrio e i relativi vantaggi conseguiti dall'adozione della normativa ISO/IEC 27701?

**R**: Senz'altro. Anzitutto, tengo a precisare che Banca Popolare di Sondrio è stata una delle prime banche in Italia ad accaparrarsi la certificazione di conformità alla normativa ISO/IEC 27701. In un mondo sempre più digitale e connesso, il tema della tutela della *privacy* riveste un ruolo prioritario per ogni tipologia di organizzazione, ancor più per quelle che operano nel settore bancario. Da sempre, la Banca è particolarmente sensibile e attenta alla tutela dei dati dei propri clienti, e con questa certificazione Banca Popolare di Sondrio rafforza il proprio impegno a implementare i più stringenti requisiti internazionali in materia di gestione della sicurezza delle informazioni e, in particolare, di tutela della *privacy* delle informazioni personali. L'ISO/IEC 27701 è uno sviluppo ed estensione della norma ISO/IEC 27001 per la gestione della sicurezza delle informazioni e stabilisce i requisiti e i controlli che tengono in considerazione non solo la normativa tecnica internazionale, ma fanno altresì esplicito riferimento al GDPR, indicando in modo chiaro e analitico gli adempimenti che competono al titolare e al responsabile del trattamento, prevedendo stabilmente anche il monitoraggio e il riesame del sistema di gestione, in un'ottica di miglioramento continuo dello stesso. Relativamente ai benefici, il PIMS è direttamente integrabile a un sistema ISMS esistente, protegge la

reputazione aziendale rassicurando i clienti e il *management* che i loro dati vengono gestiti in modo responsabile con le tecnologie più sofisticate senza violare la *privacy* degli interessati, fornisce una chiara visibilità dovuta alla corretta gestione dei dati, e la certificazione è sinonimo di conformità alla normativa europea.

**D**: L'impresa ha adottato altri *standard* normativi della serie ISO ottenendo le relative certificazioni in ambiti differenti alla protezione dei dati?

**R**: Sì, su base volontaria le varie divisioni della Banca operano per ottenere le certificazioni che ritengono utili. In particolare, si può citare ISO 9001. La banca è infatti, tradizionalmente impegnata nel perseguimento di *standard* qualitativi elevati, con l'obiettivo di massimizzare l'efficienza e soddisfare al meglio la clientela.

**D**: L'impresa ha adottato altri comportamenti e pratiche socialmente responsabili in altri ambiti oltre che in materia di *privacy*?

**R**: La Banca, in conformità al Decreto Legislativo n. 254/2016, ha redatto la dichiarazione consolidata di carattere non finanziario (DNF) pubblicata sul sito istituzionale della stessa. Nello specifico, la DNF ha il fine di assicurare la comprensione delle *policy*, del modello organizzativo, dei rischi e degli indicatori di *performance* e dei relativi risultati del gruppo rispetto, in particolar modo, agli aspetti sociali e attinenti alla gestione del personale, alla lotta contro la corruzione attiva e passiva e al rispetto dei diritti umani. Inoltre, la Banca ha da tempo adottato il "modello di organizzazione, gestione e controllo" ai sensi del decreto legislativo n. 231 dell'8

luglio 2001 e successive modificazioni e integrazioni e ha recentemente aggiornato anche il codice etico aziendale, allineando i comportamenti attesi in relazione al rispetto delle più recenti normative.

**D**: Come viene comunicata la *privacy policy* agli *stakeholder* dell'impresa?

**R**: Attraverso i normali mezzi di comunicazione delle prassi operative, esempio le circolari aziendali e inoltre sul tema è stato effettuato un piano continuo di formazione che prevede corsi ai neoassunti, corsi a tutto il personale, tramite corsi *online* interni, e corsi su aspetti specifici, esempio sul registro dei trattamenti e nomine a responsabile del trattamento esterno erogati alle figure d'interesse.

**D**: L'impresa ha ottenuto vantaggi di *marketing* derivanti da comportamenti socialmente responsabili in materia di *privacy*?

**R**: È difficile poter misurare eventuali vantaggi di *marketing* a seguito di comportamenti socialmente responsabili, tuttavia, a nostro avviso, tutto ciò che può rispondere a valori etici, a cui la banca crede e imposta da sempre la propria attività, può portare solamente benefici ai processi aziendali e allo sviluppo dell'istituto.

# RIFERIMENTI


ABBAGNANO N. (1961), *Dizionario di filosofia*, UTET, Torino.

ACCIAI R., ANGELETTI S. (2019), *Il DPO protagonista dell'innovazione. Il responsabile della protezione dei dati tra competenze e certificazioni*, Aracne Editore, Roma.

ACKERMAN R., BAUER R. A. (1976), *Corporate Social Responsiveness: Modern Dilemma*, Reston VA, Reston Publishing Company.

AGUILERA R.V., RUPP D., WILLIAMS C.A., GANAPATHI J. (2007), *Putting the S back in CSR: a multilevel theory of social change in organizations*, Academy of Management Review, 32(3), 836–863.

ALJERAISY A., RANA O., PERERA C. (2020), *A Systematic Analysis of Privacy Laws and Privacy by Design Schemes for the Internet of Things: A Developer's Perspective*, HAL archives ouvertes, Pré-publication.

ALPA G. (1998), *La disciplina dei dati personali: note esegetiche sulla Legge 31 dicembre 1996, n. 675 e successive modifiche*, Seam Edizioni, Roma.

ALPA G. (2019), *La "proprietà" dei dati personali*, in ZORZI GALGANO N. (a cura di) (2019), *Persona e mercato dei dati. Riflessione sul GDPR,* Cedam, Padova.

AMANTEA A. (2020), *Definizione di PMI: caratteristiche e classificazione delle piccole e medie imprese. Qual è la definizione di PMI e quali caratteristiche si devono rispettare (fatturato e occupati) per rientrare fra le piccole e medie imprese*, Lavoro e Diritti: https://www.lavoroediritti.com/soldi-e-diritti/definizione-pmi-piccole-medie-imprese.

AMERICAN MARKETING ASSOCIATION (AMA): https://www.ama.org/the-definition-of-marketing-what-is-marketing/.

ANDERSON J. (1987), *Can social responsibility be handled as a corporate investment?,* Business Horizons, 24-25.

ANGELINI R. (2018), *Intelligenza Artificiale e governance. Alcune riflessioni di sistema*, in PIZZETTI F. (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, G. Giappichelli Editore, Torino.

ARNABOLDI N., FERRARA F. G. (2019), *Come compilare il registro delle attività di trattamento dati*, Maggioli Editore, Santarcangelo di Romagna.

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*.

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Working document 01 2011 on the current EU personal data breach framework and recommendations for future policy developments*, WP 184, adottato il 5 aprile 2011.

ASHRAFI M., ACCIARO M., WALKER T. R., MAGNAN G. M., ADAMS M. (2019), *Corporate sustainability in Canadian and US maritime ports*, Journal of Cleaner Production, 220, 386-397.

ASHRAFI M., ADAMS M., WALKER T. R., MAGNAN G. M. (2018), *How corporate social responsibility can be integrated into corporate sustainability: a theoretical review of their relationships*, International Journal of Sustainable Development & World Ecology, 25 (8), 672-682.

ASHWORTH L., FREE C. (2006), *Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns*, Journal of Business Ethics, 67, 107-123.

ATHEY S., CATALINI C., TUCKER C. (2017), *The digital privacy paradox: small money, small costs, small talk*, National Bureau of Economic Research, Cambridge, MA, Working Paper 23488.

AVITABILE A. (2017), *Il data protection officer*, in *Il nuovo Regolamento sulla privacy e sulla protezione dei dati personali*, diretto da FINOCCHIARO G. D., Zanichelli, Bologna.

AWAZU Y., DESOUZA K. C. (2004), *The knowledge chiefs: CKOs, CLOs and CPOs*, European Management Journal, 22(3), 339–344.

BAI X., CHANG J. (2015), *Corporate social responsibility and firm performance: The mediating role of marketing competence and the moderating role of market environment*, Asia Pacific Journal of Management, 32, 505-530.

BAKER A. (2020), *ISO/IEC 27701 and the privacy information management system requirements*, IT Governance European Blog: https://www.itgovernance.eu/blog/en/iso-iec-27701-and-the-privacy-information-management-system-requirements.

BALDASSARRE A. (1997), *Diritto della persona e valori costituzionali*, G. Giappichelli Editore, Torino.

BALLUCHI F., FURLOTTI K. (a cura di) (2017), *La responsabilità sociale delle imprese. Un percorso verso lo sviluppo sostenibile. Profili di governance e di accountability*, G. Giappichelli Editore, Torino.

BANCA POPOLARE DI SONDRIO: https://www.popso.it/.

BANSAL P., DESJARDINE M. R. (2014), *Business sustainability: It is about time*, Strategic Organization, 12(1), 70-78.

BARNARD C. I. (1938), *The Functions of the Executive*, Cambridge MA, Harvard University Press.

BARNETT M. L. (2007), *Stakeholder influence capacity and the variability of financial returns to corporate social responsibility*, Academy of Management Review, 32.

BARNEY J. B., HANSEN M. H. (1994), *Trustworthiness as a source of competitive advantage*, Strategic Management Journal, 15.

BAROCAS S., SELBST A.D. (2016), *Big Data's Disparate Impact*, 104 California Law Review, 673.

BASSANI M., BIFULCO R., D'ACQUISTO G., NALDI M., POLLICINO O., PIZZETTI F. (a cura di) (2018), *Intelligenza artificiale, protezione dei dati personali e regolazione,* G. Giappichelli Editore, Torino.

BENEDETTI D., *IA e (in)sicurezza informatica*, in PIZZETTI F. (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, G. Giappichelli Editore, Torino.

BERENS G., VAN RIEL C. B. M., VAN BRUGGEN G. H. (2005), *Corporate Associations and Consumer Product Responses: The Moderating Role of Corporate Brand Dominance*, Journal of Marketing, 69(3), 35-48.

BERNARDI N., CICCIA MESSINA A. (2017), *Privacy e Regolamento Europeo*, IPSOA, Milano.

BESCHORNER T. (2013), *Creating Shared Value: The One-Trick Pony Approach*, Business Ethics Journal Review, 1(17), 106–112.

BHATTACHARYA C. B., SMITH N. C., VOGEL D. (2004), *Integrating social responsibility and marketing strategy: An introduction*, California Management Review, 47(1), 5-8.

BIASIOTTI A. (2018), *Il nuovo regolamento europeo sulla protezione dei dati. Una guida pratica alla nuova privacy e ai principali adempimenti del Regolamento UE 2016/679, aggiornata al D.lgs. 101/2018*, EPC Editore, Roma, IV edizione.

BILOTTA F. (1999), *L'emersione del diritto alla privacy*, in CLEMENTE A. (a cura di), *Privacy*, Cedam, Padova.

BINCOLETTO G. (2019), *La privacy by design. Un'analisi comparata nell'era digitale*, Aracne Editrice, Roma.

BLOOM P. N., HOEFFLER S., KELLER K. L., BASURTO C. E. (2006), *How Social-Cause Marketing Affects Consumer Perceptions*, MIT Sloan Management Review 47(2), 49-55.

BOBBIO N. (1990), *L'età dei diritti*, Giulio Einaudi Editore, Torino.

BOWEN H. R. (1953), *Social responsibilities of the businessmen*, New York, Harper & Row.

BRANDEIS L.D., WARREN S. (1890), *The Right to Privacy*, Harward Law Review, 4, 193- 220.

BRAUN V., CLARKE V. (2006), *Using thematic analysis in psychology*, Qualitative Research in Psychology, Vol. 3, No. 2, pp. 77–101

BRAVO F. (2018), *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Cedam, Padova.

BRENNER M. (a cura di) (1980), *Social method and social life*, Academic Press Inc, New York.

BRITISH STANDARDS INSTITUTION (2019), *ISO/IEC 27701 Privacy Information Management Your implementation guide*.

BS10012:2017 – *Data protection. Specification for a personal information management system*:
https://shop.bsigroup.com/products/data-protection-specification-for-a-personal-information-management-system

BUCHHOLZ R. A. (1991), *Corporate responsibility and the good society: From economics to ecology*, Business Horizons, 34(4), 19-31.

BURKE L., LOGSDON J. M. (1996), *How corporate social responsibility pays off*, Long Range Planning, 29(4), 495–502.

BUSIA G. (2019), *Il ruolo dell'autorità indipendente per la protezione dei dati personali*, in ZORZI GALGANO N. (a cura di) (2019), *Persona e mercato dei dati. Riflessione sul GDPR,* Cedam, Padova.

BUTTARELLI G. (1997), *Banche dati e tutela della riservatezza*, Giuffrè Editore, Milano.

CALIFANO L., COLAPIETRO C. (a cura di) (2017), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale Scientifica, Napoli.

CAMARDI C. (2019), *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali*, Giustizia Civile, 3, p. 499.

CAMERA DEI DEPUTATI (2021), *Documentazione Parlamentare*, *Il nuovo approccio europeo all'Intelligenza Artificiale*.

CAROLI M. G., TANTALO C. (a cura di) (2010), *La responsabilità sociale d'impresa nel quadro delle "linee guida OCSE destinate alle imprese multinazionali". Un focus sulle piccole e medie imprese*, Rapporto di ricerca con il patrocinio dell'Istituto per la promozione industriale (IPI) e del Ministero dello Sviluppo Economico (MiSE), Roma, Luiss Business School, p. 1-243.

CARROLL A. B. (1979), *A three-dimensional conceptual model of corporate performance*, Academy of Management Review, 4(4), 497-505.

CARROLL A. B. (1991), *The pyramid of corporate social responsibility: Toward the moral management of organizational stakeholders*, Business Horizons, 34(4), 39-48.

CARROLL A. B. (1998), *The four faces of corporate citizenship*, Business and Society Review, 100(1), 1-7.

CARROLL A. B. (1999), *Corporate social responsibility: Evolution of a definitional construct*, Business & Society 38(3), 268-295.

CARTA DEI DIRITTI DELL'UNIONE EUROPEA (CARTA DI NIZZA): https://www.europarl.europa.eu/charter/pdf/text_it.pdf.

CERANA N. (a cura di) (2004), *Comunicare la responsabilità sociale. Teorie, modelli, strumenti e casi d'eccellenza*, FrancoAngeli, Milano.

CERQUITELLI T., QUERCIA D., PASQUALE F. (2017), *Transparent Data Mining for Big and Small Data*, Springer International, New York.

CHAUDHRI V. A. (2006), *Organising global CSR: a case study of Hewlett-Packard's e-inclusion initiative*, Journal of Corporate Citizenship, 23, 39–51.

CHRISTENSEN C. M., BAUMANN H., RUGGLES R., STADTLER T. M. (2006), *Disruption Innovation for Social Change*, Harvard Business Review, 94-101.

CHUNG L., WEI C. (2017), *The Impact Effect of Corporate Governance and Corporate Social Responsibility on Company Performance After the Financial Tsunami*, Asian Journal of Economic Modelling, 5(4), 465-479.

CHURCH D.J. (2012), *Neuroscience in the Courtroom: An International Concern*, William & Mary Law Review, 53(5), pp. 1825–1854.

CICCIA MESSINA A. (2016), *Regolamento Privacy UE: pro e contro del nuovo sistema sanzionatorio*, Rapporto di lavoro in IPSOA Quotidiano, pp. 1-3: https://www.ipsoa.it/documents/lavoro-e-previdenza/rapporto-

di-lavoro/quotidiano/2016/10/19/regolamento-privacy-ue-pro-e-contro-del-nuovo-sistema-sanzionatorio.

CISCO SYSTEMS INC. (2020), *Data Privacy Benchmark Study*: https://www.cisco.com/c/dam/global/en_uk/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf

CLARKSON M. B. E. (1995), *A Stakeholder Framework for Analyzing and Evaluating Corporate Social Performance*, The Academy of Management Review, 20(1), 92-117.

CODICE DEL CONSUMO, decreto legislativo 6 settembre 2005, n. 206.

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.

COLAIANNI N. (2000), *Tutela della personalità e diritti della coscienza*, Cacucci Editore, Bari.

COLLINS M., SYKES W. (1985), *Telephone interviewing on a survey of social attitudes*, in *Survey methods newsletter*.

COMELLINI S. (2018), *Il responsabile della protezione dei dati (Data Protection Officer-DPO)*, Maggioli Editore, Santarcangelo di Romagna.

COMMISSIONE EUROPEA, Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *L'intelligenza artificiale per l'Europa,* COM(2018) 237, 25 aprile 2018.

COMMISSIONE EUROPEA, comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Bruxelles, 25 ottobre 2011. COM (2011) 681 definitivo.

COMMISSIONE EUROPEA, *Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, COM (2021) 206 del 21.04.2021.

COMMISSIONE EUROPEA, *Digital single market-Big Data*: *ec.europa.eu*.

COMMISSIONE EUROPEA, raccomandazione n. 2003/361/CE del 6 maggio 2003 (in Gazzetta Ufficiale delle Comunità europee L 124 del 20 maggio 2003), recepita dall'ordinamento italiano con decreto del Ministro delle attività produttive del 18 aprile 2005.

COMPAGNONI F., ALFORD H. (2008), *Fondare la responsabilità sociale d'impresa. Contributi dalle scienze umane e dal pensiero sociale cristiano*, Città Nuova Editrice, Roma.

CONVENZIONE DI STRASBURGO del 1981, Convenzione 108 del Consiglio d'Europa: http://www.privacy.it/archivio/convstrasb.html.

CONVENZIONE EUROPEA PER LA SALVAGUARDIA DEI DIRITTI DELL'UOMO E DELLE LIBERTÀ FONDAMENTALI.

COOL A. (2018), *Europe's Data Protection Law Is a Big, Confusing Mess*, The New York Times.

COOLEY T. C. (1888), *A Treatise on the Law of Torts or the Wrongs which Arise Independent of Contract*, Callaghan & Company, Chicago, IL.

COSTITUZIONE DELLA REPUBBLICA ITALIANA.
https://www.cortecostituzionale.it/documenti/download/pdf/Costituzione_della_Repubblica_italiana.pdf.

CRESWELL J.W. (1998), *Qualitative inquiry and research design: Choosing among five traditions*, Thousand Oaks, CA, Sage.

CRESWELL J.W. (2009), *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, Thousand Oaks, CA, Sage, Third Edition.

CUFFARO V. (2018), *Quel che resta di un codice: il D.Lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del codice della privacy al regolamento sulla protezione dei dati*, Corriere giuridico, 10, p. 1181 e ss.

CUFFARO V., D'ORAZIO R., RICCIUTO V. (a cura di) (2019), *I dati personali nel diritto europeo*, G. Giappichelli Editore, Torino.

CULNAN M. J., ARMSTRONG P. K. (1999), *Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation*, Organization Science, 10(1), 104–115.

D.lgs. 9 aprile 2008, n. 81, art. 2, comma 1, par. ff - Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro. (GU Serie Generale n.101 del 30-04-2008 - Suppl. Ordinario n. 108).

D'ACQUISTO G., NALDI M. (2017), *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, G. Giappichelli Editore, Torino.

DAVIS K. (1960), *Can business afford to ignore social responsibilities?*, California Management Review, 2(3), 70-76.

DAVIS K. (1967), *Understanding the Social Responsibility Puzzle*, Business Horizons, 10(4), 45-50.

DAVIS K. (1973), *The case for and Against Business Assumption of Social responsibilities*, The Academy of Management Journal, 16(2), 312-322.

DAVIS K., BLOMSTROM R. L. (1966), *Business and its Environment*, New York, McGraw Hill.

DE GIROLAMO S., D'ANSELMI P. (2017), *La responsabilità sociale delle organizzazioni. L'impresa sostenibile e lo sviluppo competitivo*, FrancoAngeli, Milano.

DE STEFANI F. (2018), *Le regole della privacy: Guida pratica al nuovo GDPR*, HOEPLI, Milano.

Decreto legislativo 10 agosto 2018, n. 101, Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) (GU Serie Generale n.205 del 04-09-2018).

Decreto legislativo 30 dicembre 2016, n. 254. Attuazione della direttiva 2014/95/UE del Parlamento europeo e del Consiglio del 22 ottobre 2014, recante modifica alla direttiva 2013/34/UE per quanto riguarda la comunicazione di informazioni di carattere non finanziario e di informazioni sulla diversità da parte di talune imprese e di taluni gruppi di grandi dimensioni. (17G00002) (GU Serie Generale n.7 del 10-01-2017.

Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" pubblicato nella Gazzetta Ufficiale n. 174 del 29 luglio 2003 - Supplemento Ordinario n. 123.

DI CARNABUCI A., CECCOLI P., DE ROSA B., MARIANI I., MINIERI C., RADAELLI P., ZAPPIA A., ZUCCHETTI A. (2018), *Privacy e dati personali: Problemi e casi pratici*, Key Editore, Milano.

DI NUNZIO A. (2020), *Due diligence e privacy: un binomio ormai imprescindibile. Perché e come verificare la compliance dell'azienda*: https://www.studiolegalestefanelli.it/it/sharingknowledge/articoli/a/due-diligence-privacy-perche-e-come-verificare-compliance-azienda.

DI RESTA F. (2018), *La nuova «privacy europea». I principali adempimenti del regolamento UE 2016/679 e profili risarcitori*, G. Giappichelli Editore, Torino.

Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio dell'11 dicembre 2018, da attuarsi entro il 21 dicembre 2020, che istituisce il codice europeo delle comunicazioni elettroniche e che tocca, con disposizioni specifiche, anche l'ambito dei dati di carattere personale.

Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali.

Direttiva (UE) 2019/771 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di vendita di beni, che modifica il regolamento (UE) 2017/2394 e la direttiva 2009/22/CE, e che abroga la direttiva 1999/44/CE.

Direttiva 1999/44/CE del Parlamento europeo e del Consiglio, del 25 maggio 1999, su taluni aspetti della vendita e delle garanzie dei beni di consumo Gazzetta ufficiale n. L 171 del 07/07/1999 pag. 0012 – 0016.
Direttiva 2006/42/CE del Parlamento europeo e del Consiglio, del 17 maggio 2006, relativa alle macchine e che modifica la direttiva 95/16/CE.

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.
DOLAN P. (2002), *The sustainability of "sustainable consumption"*, Journal of Macromarketing, 22(2), 170-181.

DONALDSON T., DUNFEE T. W. (1994), *Toward a unified conception of business ethics: Integrative social contracts theory*, Academy of Management Review, 19(2), 252-284.

DRUCKER P. F. (1954), *The practice of management*, New York, Harper & Row Publishers.

DUNFEE T. W., DONALDSON T. (1999), *Social Contract Approaches to Business Ethics: Bridging the "Is-Ought" Gap* in FREDERICKS R. (a cura di), *A companion to business ethics*, Oxford, Blackwell.

EDELMAN D. C., SINGER M. (2015), *Competing on customer journeys*, Harvard Business Review, 93(11), 88-100.

EDPB, *Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation 2016/679*, adottate il 4 dicembre 2018.

EILBIRT H., PARKET R. (1973), *The practice of business: The current status of corporate social responsibility*, Business Horizons, 16(4), 5-14.

ELKINGTON J. (1994), *Towards the Sustainable Corporation: Win-Win-Win Business Strategies for Sustainable Development*, California Management Review, 36(2), 90-100.

EUROPA 2020. *Una strategia per una crescita intelligente, sostenibile e inclusiva*. Bruxelles, 3 marzo 2010. COM (2010) 2020 definitivo.

EUROPEAN DATA PROTECTION BOARD: https://edpb.europa.eu/edpb_en.

FABIANO N. (2019), *GDPR & privacy: consapevolezza e opportunità. Analisi ragionata della protezione dei dati personali tra etica e cybersecurity*, goWare, Firenze.

FABIANO N. (2020), *GDPR & Privacy: consapevolezza e opportunità. L'approccio con il Data Protection and Privacy Relationships Model (DAPPREMO)*, goWare, Firenze.

FARALLI C. (2019), *Il diritto alla privacy. Profili storico-filosofici*, in ZORZI GALGANO N. (a cura di) (2019), *Persona e mercato dei dati. Riflessione sul GDPR,* Cedam, Padova.

FAYYAD U.M., PIATETSKY-SHAPIRO G., SMYTH P. (1996), *From data mining to knowledge discovery: an overview*, in FAYYAD U.M., *Advances in Knowledge Discovery and Data Mining*, AAAI Press, Menlo Park, CA.

FEDERPRIVACY: https://www.federprivacy.org/.

FERNÁNDEZ B., SOUTO F. (2009), *Crisis and Corporate Social Responsibility: Threat or Opportunity?*, International Journal of Economic Sciences and Applied Research, 2(1), 36-50.

FINOCCHIARO G. D. (2017), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli Editore, Bologna.

FINOCCHIARO G. D. (2017), *Il quadro d'insieme*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, diretto da FINOCCHIARO G. D., Zanichelli, Bologna.

FITCH H. G. (1976), *Achieving Corporate Social Responsibility*, Academy of Management Review, 1(1).

FLORIDI L. (2009), *Infosfera. Etica e filosofia nell'età dell'informazione*, G. Giappichelli Editore, Torino.

FLORIDI L. (2017), *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, Milano, 2017.

FOMBRUN C., SHANLEY M. (1990), *What's in a name? Reputation building and corporate strategy*, Academy of Management Journal, 33, 233–258.

FRANCESCHELLI V. (1998), *La tutela della privacy informatica: problemi e prospettive*, Giuffrè Editore, Milano.

FREDERIK W. C. (1960), *The growing concern over business responsibility*, California Management Review, 2(4), 54-61.

FREDERICK W. C. (1986), *Toward CSR3: Why Ethical Analysis is Indispensable and Unavoidable in Corporate Affairs*, California Management Review, 28(2), 126-141.

FREDERICK W. C. (1994), *From CSR1 to CSR2: The maturing of business-and-society thought*, Business & Society, 33(2), 150-164.

FREDERICK W. C. (1998), *Moving to CSR4: what to pack for the trip*, Business and Society, 37(1), 40-59.

FREDERICK W. C. (2006), *Corporation, Be Good! The Story of Corporate Social Responsibility*, Indianapolis, IN, Dog Ear Publishing.

FREEMAN R. E. (1984), *Strategic Management: A Stakeholder Approach*, Boston, Pitman.

FREY J.H. (1989), *Survey research by telephone*, London.

FRIEDMAN M. (1962), *Capitalism and Freedom*, University of Chicago Press.

FUKUKAWA K. E MOON J. (2004), *A Japanese model of corporate social responsibility? A study of website reporting*, Journal of Corporate Citizenship, 16, 45–59.

GANGI F., MUSTILLI M. (2018), *La responsabilità sociale d'impresa. Principi e pratiche*, Egea, Milano.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI: https://www.garanteprivacy.it.

GIACOMETTI A. (2013), *Il marketing sostenibile: dal dire al fare business, responsabilmente. Principi, metodi e strumenti per innovare*

*col Marketing la Responsabilità Sociale d'Impresa (CSR) in chiave sostenibile ed etica*, Maggioli Editore, Santarcangelo di Romagna.

GIANNANTONIO E., LOSANO G., ZENO-ZENCOVICH V. (a cura di) (1999), *La tutela dei dati personali. Commentario alla legge n. 675/96*, seconda edizione, Cedam, Padova.

GIANNARAKIS G., THEOTOKAS I. (2011), *The Effect of Financial Crisis in Corporate Social Responsibility Performance*, International Journal of Marketing Studies, 3(1), 1-10.

GODFREY P. C., MERRILL C. B., HANSEN J. M. (2009), *The relationship between corporate social responsibility and shareholder value: an empirical test of the risk management hypothesis*, Strategic Management Journal, 30(4), 425-445.

GRECO L. (2017), *I ruoli: titolare e responsabile*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, diretto da FINOCCHIARO G. D., Zanichelli, Bologna.

GREENING D. W., TURBAN D. B. (2000), *Corporate social performace as a competitive advantage in attracting a quality workforce*, Business and Society, 39, 254-280.

GROW B., *The Debate over Doing Good*, BusinessWeek, 15 agosto 2005.

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, parere 3/2010 sul principio di responsabilità, adottato il 3 luglio 2010.

GRUSCHKA N., MAVROEIDIS V., VISHI K., JENSEN M. (2018), *Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR*, IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, pp. 5027-5033.

HABERMAS J. (1967), *Zur logik der Sozialwissenschaften*, Tübingen. (Tr. it.: *Agire comunicativo e logica delle scienze sociali*, il Mulino, Bologna, 1980).

HALLINAN D., SCHÜTZ P., FRIEDEWALD M., DE HERT P. (2014), *Neurodata and Neuroprivacy: Data Protection Outdated?*, Surveillance & Society, 12(1), 55-72.

HARRIS S. (2010), *All-In-One CISSP Guide*, 5th Edition, McGraw Hill, USA.

HEALD M. (1957), *Management's Responsibility to Society: The Growth of an Idea*, Business History Review, 31(4), 375-384.

HOEFFLER S., KELLER K. L. (2002), *Building Brand Equity through Corporate Societal Marketing*, Journal of Public Policy & Marketing, 21(1), 78-89.

HOSMER L. T. (1991), *The Ethics of Management*, Irwin, Homewood, IL.

HOSMER L. T. (1994), *Strategic Planning as if Ethics mattered, Strategic Management Journal*, 15.

HUNT S. D. (1983), *General theories and the fundamental explananda of marketing*, Journal of Marketing, 47(4), 9-17, p. 13.

IASELLI M. (2018), *Manuale operativo del DPO (Data Protection Officer)*, Maggioli Editore, Santarcangelo di Romagna.

IASELLI M. (2019), *Sanzioni e responsabilità in ambito GDPR*, Giuffrè Editore, Milano.

IL POST (2021), *Come l'Europa vuole regolamentare le intelligenze artificiali La Commissione Europea ha presentato una proposta molto articolata e ambiziosa sulle tecnologie al centro del nostro futuro*: https://www.ilpost.it/2021/04/22/commissione-europea-intelligenza-artificiale/.

INTERNATIONAL DATA CORPORATION (2020), *Global DataSphere forecast:* https://www.idc.com/getdoc.jsp?containerId=IDC_P38353.

INTERNET SOCIETY (2015), *The Internet of Things: An Overview.*

IPSOA REDAZIONE (2019), *Contratti di vendita di beni e di contenuto digitale: l'UE adotta nuove norme.*

ISO/IEC 27001:2013 *Information technology — Security techniques — Information security management systems — Requirements*: https://www.iso.org/standard/54534.html.

ISO/IEC 27701:2019 *Security techniques — Extension to* ISO/IEC 27001 *and* ISO/IEC 27002 *for privacy information management — Requirements and guidelines*:https://www.iso.org/standard/71670.html.

ISO/IEC 29100:2011 *Information technology — Security techniques — Privacy framework*: https://www.iso.org/standard/45123.html.

IT GOVERNANCE (2019), *Green paper – ISO 27701 Privacy information management systems*, IT Governance Publishing.

JACOB C. K. (2012), *The Impact of Financial Crisis on Corporate Social Responsibility and Its Implications for Reputation Risk Management*, Journal of Sustainability Science and Management 2(2), 259-275.

JANNELLI R., MENEGUZZO M., FIORANI G. (2012), *CSR 2.0 proattiva e sostenibile. Tra mercati globali e gestione della crisi*, Egea, Milano.

JEURISSEN R. (2000), *John Elkington, Cannibals With Forks: The Triple Bottom Line of 21st Century Business*, Journal of Business Ethics, 23(2), 229-231.

JOHN MAYNARD KEYNES (1923), *A Tract on Monetary Reform*.

JOHNSON H. L. (1971), *Business in contemporary society: Framework and issues*. Belmont CA, Wadsworth Pub. Co.

JOHNSSÉN F., EDVARDSEN S. (2020), *Data Protection Officer,* BCS, The Chartered Institute for IT, Londra.

JONES T. M. (1980), *Corporate Social Responsibility Revisited, Redefined*, California Management Review, 22(3), 59-67.

JONES T. M. (1995), *Instrumental stakeholder theory: a synthesis of ethics and economics*, Academy of Management Review, 20(2), 404–437.

KAYWORTH T., BROCATO L., WHITTEN D. (2005), *What is a chief privacy officer?*, Communications of AIS, 16, 110–126.

KHAMESRA S. (2021), *Implementing ISO 27701:2019 PIMS – Two common fallacies*: https://pricoris.com/implementing-iso-27701/.

KOTLER P., KELLER K. L., ANCARANI F., COSTABILE M. (2017), *Marketing Management*, Pearson Italia, quindicesima edizione traduzione italiana, Milano. Edizione originale: KOTLER P. (1967), *Marketing Management: Analysis, Planning, and Control*, Prentice Hall, Englewood Cliffs, NY.

KRAFFT M., ARDEN C. M., VERHOEF P. C. (2017), *Permission Marketing and Privacy Concerns—Why Do Customers (Not) Grant Permissions?*, Journal of Interactive Marketing, 39, 39-54.

KU H. H., YANG P. H., CHANG C. L. (2018), *Reminding customers to be loyal: does message framing matter?*, European Journal of Marketing, 52(3/4), 783-810.

LANTOS G. (2001), *The boundaries of strategic corporate social responsibility*, The Journal of Consumer Marketing, 18(7), 595-630.

LAVRAKAS P.J. (1987), *Telephone survey methods. Sampling, selection and supervision*, London.

Legge n. 675 del 31 dicembre 1996, Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali (testo consolidato con il d.lgs. 28 dicembre 2001, n. 467) (Pubblicato sulla Gazzetta Ufficiale n. 5 dell´8 gennaio 1997 - Suppl. Ordinario n. 3) Legge abrogata ai sensi dell'articolo 183, comma 1, lettera a), del Codice in materia di protezione dei dati personali.

LEVITT T. (1958), *The Dangers of Social Responsibility*, Harvard Business Review, 36, 41-50.

LIBRO BIANCO sull'intelligenza artificiale – *Un approccio europeo all'eccellenza e alla fiducia*, 19 febbraio 2020. Bruxelles, 19.2.2020 COM(2020) 65 *final*.

LIBRO VERDE, *Promuovere un quadro europeo per la responsabilità sociale delle imprese* presentato dalla Commissione delle Comunità Europee. Bruxelles, 18 luglio 2001. COM (2001) 366 definitivo.

LICHTENSTEIN D. R., DRUMWRIGHT M. E., BRAIG B. M. (2004), *The Effect of Corporate Social Responsibility on Customer Donations to Corporate-Supported Nonprofits*, Journal of Marketing, 68(4), 16-32.

LITTLEFIELD M. (2008), *Constructing the Organ of Deceit*, Science, Technology, & Human Values, 34 (3), 365–392.

LOHR S. (2012). *Sure, Big Data is Great. But so is intuition*, The New York Times: https://www.nytimes.com/2012/12/30/technology/big-data-is-great-but-dont-forget-intuition.html.

LOSITO G. (1988), *Metodi e tecniche della ricerca sociale empirica sull'emittenza*, in LIVOLSI M. e ROSITI F. (a cura di), *La ricerca sull'industria culturale*, Carocci Editore, Roma.

LOSITO G. (1998), *Sociologia. Un'introduzione alla teoria e alla ricerca sociale*, Carocci Editore, Roma.

MAGLIO M., POLINI M., TILLI N. (2017), *Manuale di diritto alla protezione dei dati personali. La privacy dopo il Regolamento UE 2016/679*, Maggioli Editore, Santarcangelo di Romagna.

MAIETTA A. (2020), *Il principio di autoresponsabilità. Il modello del Data Protection Officer*, G. Giappichelli Editore, Torino.

MAIGNAN I., FERRELL O. C. (2004), *Corporate social responsibility and marketing: An integrative framework*, Journal of the Academy of Marketing Science, 32(1), 3-19.

MAITLIS, S. (2012), *Narrative analysis*, in SYMON G., CASSELL C. (eds), *Qualitative Organizational Research: Core Methods and Current Challenges*, London, Sage.

MANNE H. G., WALLICH H. C. (1972), *The modern corporation and social responsibility*, Washington, American Enterprise Institute for Public Policy Research.

MANTELERO A. (2017*), Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva (Artt. 32-39)*, in FINOCCHIARO G. D. (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna.

MANTELERO A. (2017), *Responsabilità e rischio nel Reg. UE 2016/679*, Le Nuove leggi civili commentate, 1, p. 144 e ss.

MANTELERO A. (2018), *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, Computer Law & Security Review, 34, 754–772.

MANTELERO A. (2018), *La privacy all'epoca dei big data*, in *Protezione e libera circolazione dei dati personali nel diritto europeo. Il regolamento generale 2016/679 (e le direttive 2016 680 e 2016 681 sul trattamento dei dati in ambito penalistico)*, CUFFARO V., D'ORAZIO R., RICCIUTO V. (a cura di), G. Giappichelli Editore, Torino.

MANTELLI DAVINI AVVOCATI ASSOCIATI INTERNATIONAL CONTRACT LAWYERS (2021), *Novità in tema di tutela e garanzie legali e commerciali dei consumatori: la nuova Direttiva UE 2019/771*: https://imantelli.eu/novita-in-tema-di-tutela-e-garanzie-legali-e-commerciali-dei-consumatori-la-nuova-direttiva-ue-2019-771/.

MARCOS E., LABRECQUE L. I., MILNE G.R. (2018), *A New Information Lens: The Self-concept and Exchange Context as a Means to Understand Information Sensitivity of Anonymous and Personal Identifying Information*, Journal of Interactive Marketing, 42, 46–62.

MARÍN L., RUIZ S., RUBIO A. (2009), *The role of identity salience in the effects of corporate social responsibility on consumer behavior*, Journal of Business Ethics, 84, 65-78.

MARRADI A. (1993), *L'analisi monovariata*, FrancoAngeli, Milano.

MARTIN K. D., BORAH A., PALMATIER R. W. (2017), *Data privacy: Effects on customer and firm performance*, Journal of Marketing, 81(1), 36-58.

MARTIN K. D., MURPHY P. E. (2017), *The role of data privacy in marketing*, Journal of the Academy of Marketing Science, 45, 135-155.

MATTHEWS S. (2015), *Neuromarketing: What Is It and Is It a Threat to Privacy?*, in CLAUSEN J., LEVY N. (eds), *Handbook of Neuroethics*, Springer, Dordrecht, pp. 1627 –1645.

MCCORMICK B. (2006), *Your Thoughts May Deceive You: The Constitutional Implications of Brain Fingerprinting Technology and How it May Be Used to Secure Our Skies*, Law & Psychology Review, 30, 171–184.

McDONOUGH J. e McDONOUGH S. (1997), *Research Methods for English Language Teachers*, London, Arnold.

McGUIRE J. W. (1963), *Business and Society*, New York, McGraw Hill.

McPHERSON H. (2014), *Data Privacy—Protecting This Asset Is a Priority*, Isaca Journal Archives: https://www.isaca.org/resources/isaca-journal/pastissues/2014/data-privacy-protecting-this-asset-is-a-priority.

McWILLIAMS A., SIEGEL D. (2001), *Corporate Social Responsibility: a theory of the firm perspective, Academy of Management Review*, 26 (1).

McWILLIAMS A., SIEGEL D., WRIGHT P. M. (2006), *Corporate social responsibility: Strategic Implications*, Journal of Management Studies, 43.

MERLI R. (2012), *La responsabilità sociale d'impresa: aspetti teorici e strumenti operativi*, Cedam, Padova.

MESSINETTI R. (2019), *Trattamento dei dati per finalità di profilazione e decisioni automatizzate*, in ZORZI GALGANO N. (a cura di) (2019), *Persona e mercato dei dati. Riflessione sul GDPR,* Cedam, Padova.

MILLS A. J., DUREPOS G., WIEBE E. (2010), *Descriptive Case Study* in *Encyclopedia of Case Study Research,* SAGE Publications, Thousand Oaks, CA.

MINTZBERG H. (1983), *The case for corporate social responsibility*, Journal of Business Strategy, 4(2), 3-15.

MOLLO F. (2019), *Gli obblighi previsti in funzione di protezione dei dati personali*, in ZORZI GALGANO N. (a cura di) (2019), *Persona e mercato dei dati. Riflessione sul GDPR,* Cedam, Padova.

MOLTENI M. (2004), *Responsabilità sociale e performance d'impresa*, Vita e Pensiero - Pubblicazioni dell'Università Cattolica del Sacro Cuore, Milano.

MOORE A.D. (2017), *Privacy, Neuroscience, and Neuro-Surveillance*, Res Publica, 23, 159–177.

MORRI L. (2009), *Storia e teorie della responsabilità sociale d'impresa. Un profilo interpretativo*, FrancoAngeli, Milano.

MURPHY P. E., LACZNIAK G. R., BOWIE N. E., KLEIN T. A. (2005), *Ethical Marketing*, Pearson, Upper Saddle River, NJ.

MURRU F. (a cura di) (2009), *Responsabilità sociale d'impresa. Il punto di vista dei lavoratori*, FrancoAngeli, Milano.

NAHAPIET J., GHOSAL S. (1998), *Social capital, intellectual capital, and the organizational advantage*, Academy of management review, 23(2).

NIGER S. (2006), *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, Padova.

NIGRO C., PETRACCA M. (2016), *La CSR dalle origini all'approccio neo-istituzionalista. Focus sui processi di isomorfismo e di decoupling*, G. Giappichelli Editore, Torino.

NORBERG P. A., HORNE D. R. (2007), *Privacy attitudes and privacy-related behavior*, Psychology and Marketing, 24(10), 829–847.

NORBERG P. A., HORNE D. R., HORNE D. A. (2007), *The privacy paradox: personal information disclosure intentions versus behaviors*, Journal of Consumer Affairs, 41(1), 100–126.

NUOVA STRATEGIA PER IL MERCATO UNICO DIGITALE IN EUROPA, COM(2015) 192 *final* del 6.5.2015.

PAGANO R. (2017), *L'organizzazione aziendale per l'implementazione del Sistema Privacy. Tutti i passi utili all'adozione di un sistema privacy conforme alle norme vigenti*, Independently published.

PANETTA R. (2019), *Il trasferimento all'estero dei dati personali*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, (a cura di) ZORZI GALGANO N., Cedam, Padova.

PARDOLESI R. (a cura di) (2003), *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè Editore, Milano.

PARLAMENTO EUROPEO (2020), *Intelligenza artificiale: Il PE getta le basi per le prime regole UE*, anteprima della sessione del 19-23 ottobre 2020.

PEARLMAN E. (2015), *The brain as site-specific surveillant performative space*, International Journal of Performance Arts and Digital Media, 11 (2), 219–234.

PELINO E. (2016), *I soggetti del trattamento*, in BOLOGNINI L., PELINO E., BISTOLFI C. (2016) (a cura di), *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè Editore, Milano.

PELLECCHIA E. (2018), *Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation*, Le nuove leggi civili commentate, 41(5), 1209 – 1235.

PELOZA J., SHANG J. (2011), *How can corporate social responsibility activities create value for stakeholders? A systematic review*, Journal of the Academic Marketing Science, 39, 117-135.

PERRINI F., TENCATI A. (2008), *Corporate social responsibility. Un nuovo approccio strategico alla gestione d'impresa*, Milano, Egea.

PETTERS J. (2020), *Data Privacy Guide: Definitions, Explanations and Legislation*, Varonis: https://www.varonis.com/blog/data-privacy/.

PFOESTL E. (a cura di) (2012), *La responsabilità sociale di impresa, sviluppo, sostenibilità ed economia sociale di mercato,* Editrice Apes, Roma.

PHELPS J., NOWAK G., FERRELL E. (2000), *Privacy concerns and consumer willingness to provide personal information*, Journal of Public Policy and Marketing, 19(1), 27–41.

PITRONE M.C. (1984), *Il sondaggio*, FrancoAngeli Editore, Milano.

PITT W., THE ELDER LORD CHATHAM (1766), in HENRY PETER BROUGHAM, Historical Sketches of statesmen Who Flourished in the Time of George III, Charles Knights & Co, Londra, 1839, vol. 1, p. 52.

PIVA A., FERRI S., SALA M. (2019), *Privacy alla luce del Regolamento Europeo UE 2016/679. Guida alla certificazione «Protezione dati personali: GDPR, Privacy e Sicurezza»*, A.I.C.A. Editore.

PIZZETTI F. (2016), *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, G. Giappichelli Editore, Torino.

PIZZETTI F. (2016), *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, G. Giappichelli Editore, Torino.

POLLACH I. (2011), *Online privacy as a corporate social responsibility: an empirical study*, Business Ethics: A European Review, 20(1), 88-102.

PORTER M. E., KRAMER M. R. (2006), *Strategy & society: the link between competitive advantage and corporate social responsibility*, Harvard Business Review, 84, 78–92.

PORTER M. E., KRAMER M. R. (2011), *The Big Idea: Creating Shared Value. How to Reinvent Capitalism—and Unleash a Wave of Innovation and Growth*, Harvard Business Review, 89(1-2), 62-77.

POST J. E. (2000), *Moving from geographic to virtual communities: global corporate citizenship in a dot.com world*, Business and Society Review, 105(1), 27–46.

PRATESI C. A. (2013), *Verso il marketing sostenibile*, in MATTIACCI A., PASTORE A. (a cura di), *Marketing. Il management orientato al mercato*, Hoepli, Milano.

REDAZIONE DNV (2021), *ISO/IEC 27701 alla Banca Popolare di Sondrio per la tutela della privacy*: https://www.dnv.it/news/iso-iec-27701-alla-banca-popolare-di-sondrio-per-la-tutela-della-privacy-194859/.

REDAZIONE PRIMA LA VALTELLINA (2021), *Certificazione ISO/IEC 27701 alla Banca Popolare di Sondrio per la tutela della privacy*: https://primalavaltellina.it/economia/certificazione-iso-iec-27701-alla-banca-popolare-di-sondrio-per-la-tutela-della-privacy/.

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la dir. 95/46/CE (Regolamento generale sulla protezione dei dati).

Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio del 23 ottobre 2018 sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE.

Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio del 14 novembre 2018 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

REGISTRO IMPRESE, *I dati ufficiali delle Camere di Commercio*: https://www.registroimprese.it/.

RICCI A. (2017), *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, Contratto e impresa. Dialoghi con la giurisprudenza civile e commerciale, 2, Cedam, pp. 587-612.

RIESSMAN C.K. (2008), *Narrative Methods for the Human Sciences*, London, Sage.

RINALDI G.M., BRESCHI M. (BIRD & BIRD LLP) (2020), *Le direttive "gemelle"*: https://www.twobirds.com/~/media/pdfs/italy/bird-bird-le-direttive-gemelle-novita-sui-contenuti-e-servizi-digitali-e-sui-contratti.pdf?la=it&hash=E43E6C32B2A9933E47114F3AB0518FC74C719D92.

Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate (2020/2012(INL)).

Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL)).

Risoluzione del Parlamento europeo del 20 ottobre 2020 sui diritti di proprietà intellettuale per lo sviluppo di tecnologie di intelligenza artificiale (2020/2015(INI)).

RODOTÀ S. (1985), *Circolazione delle informazioni e protezione dei dati personali*, in AA.VV., *Il diritto delle comunicazioni di massa. Problemi e tendenze*, a cura di ROPPO V., Cedam, Padova.

RODOTÀ S. (1991), *Privacy e costruzione della sfera privata. Ipotesi e prospettive*, Politica del diritto, XXII, pp. 525 ss.

RODOTÀ S. (1995), *Tecnologie e diritti*, il Mulino, Bologna.

RODOTÀ S. (1997), *Controllo e riservatezza a garanzia della privacy ma senza i "lacci" della Burocrazia*, Guida al Diritto.

RODOTÀ S. (1997), *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, Rivista critica del diritto privato, 4, pp. 583 ss.

RODOTÀ S. (2004), *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza Editore, Roma-Bari.

RODOTÀ S. (2012), *Il diritto di avere diritti*, Laterza Editore, Roma-Bari.

ROSKIES A.L. (2015), *Mind Reading, Lie Detection, and Privacy*, Handbook of Neuroethics.

RUSCONI G. (2013), *Il bilancio sociale delle imprese: economia, etica e responsabilità sociale dell'impresa*, Ediesse, Roma.

SALA M. (2018), *Privacy. Guida alla lettura del Regolamento (UE) 2016/679 sulla protezione dei dati e del Codice Privacy italiano*, G. Giappichelli Editore, Torino.

SANCLEMENTE J. C. (2012), *Marketing y la RSE. Lo social como estrategia de marketing*, in RAUFFLET E., LOZANO J. F., BARRERA E., GARCIA C. (Eds.), *Responsabilidad Social Empresarial*, pp. 145-156, México: Pearson Educación.

SANCLEMENTE-TÉLLEZ J. C. (2017), *Marketing and Corporate Social Responsibility (CSR). Moving between broadening the concept of marketing and social factors as a marketing strategy*, Spanish Journal of Marketing, 21(1), 4-25.

SAUNDERS M., LEWIS P., THORNHILL A. (2016), *Research Methods for Business Students*, Pearson Education Limited, London, Seventh edition.

SCARCELLA PRANDSTRALLER S. (a cura di) (2013), *Teorie e tecniche della responsabilità sociale d'impresa*, Di Virgilio Editore, Roma.

SCIARELLLI S., SCIARELLI M. (2018), *Il governo etico d'impresa*, Cedam, Padova.

SELZNICK P. (1957), *Leadership in Administration: a Sociological Perspective*, New York, Harper & Row Publishers.

SEN S., BHATTACHARYA C. B. (2001), *Does doing good always lead to doing better? consumer reactions to corporate social responsibility*, Journal of Marketing Research, XXXVIII, 225-243.

SETHI S. P. (1975), *Dimensions of Corporate Social Performance: An Analytical Framework*, California Management Review, 17(3), 58-64.

SHARFMAN M. P., PINKSTON T. S. E SIGERSTAD T. D. (2000), *The effects of managerial values on social issues evaluation: an empirical examination*, Business and Society, 39(2), 144–182.

SHEEHAN K. B. (2002), *Toward a typology of internet users and online privacy concerns*, The Information Society, 18(1), 21–32.

SHIPMAN A., WATKINS S. (2020), *ISO/IEC 27701:2019: An introduction to privacy information management*, Ely, Cambridgeshire, United Kingdom: IT Governance Publishing.

SICA S. (2016), *Verso l'unificazione del diritto europeo alla tutela dei dati personali?*, La nuova disciplina europea della privacy, SICA S., D'ANTONIO V., RICCIO G. M. (a cura di), Cedam, Padova.

SIMCIC P., BELLIU A. (2001), *Corporate social responsibility and cause-related marketing: An overview*, International Journal of Advertising, 20, 207-222.

SIMMONS C. J., BECKER-OLSEN K. L. (2006), *Achieving Marketing Objectives through Social Sponsorships*, Journal of Marketing, 70(4), 154-169.

SIMON H. A. (1947), *Administrative Behaviour: A Study of the Decision Making Processes in Administrative Organisation*, New York, Macmillan Company.

SMITH A. (1776), *An Inquiry into the Nature and Causes of the Wealth of Nations*.

SMITH N. C., QUELCH J. A. (1996), *Ethics in Marketing*, McGraw-Hill, New York.

Special Report: *Corporate Social Responsibility*, The Economist, 17 gennaio 2018.

STAZI A. (2019), *Automazione contrattuale e "contratti intelligenti". Gli smart contracts nel diritto contrattuale comparato*, G. Giappichelli Editore, Torino.

STUDIO LEGALE STEFANELLI (2019), *Mercato unico digitale: la nuova normativa per la fornitura di servizi online dell'Unione Europea*: https://www.studiolegalestefanelli.it/it/approfondimenti/mercato-unico-digitale-nuova-normativa-per-fornitura-di-servizi-online-ue/#_ftn2.

TEE E., ASARE L. B., OPOKU R. T., TABITHA O. (2017), *The Effect of the 2008 Financial Crisis on Corporate Social Responsibilities: Evidence from Multinational Companies*, Research Journal of Finance and Accounting, 8(16), 20-30.

THE COMMITTEE ON SCIENCE AND LAW (2005), *Are Your Thoughts Your Own?: 'Neuroprivacy' and the Legal Implications of Brain Imaging,* The Record of the Association of the Bar of the City of New York, 60(2), pp. 407–437.

THE ECONOMIST (2017), *Data is giving rise to a new economy - Fuel of the future*: https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy.

TOIATI M. (2019), *ISO 27701 per la protezione dei dati personali: realizzare un Privacy Information Management System*, Cyber Security 360: https://www.cybersecurity360.it/legal/privacy-dati-personali/iso-27701-per-la-protezione-dei-dati-personali-realizzare-un-privacy-information-management-system/.

TOSI E. (2019), *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale. Oggettivazione del rischio e riemersione del danno morale con funzione deterrente-sanzionatoria alla luce dell'art. 82 GDPR*, Giuffrè Editore, Milano.

TRATTATO SUL FUNZIONAMENTO DELL'UNIONE EUROPEA: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:it:PDF.

TRECCANI ENCICLOPEDIA – FIDELI R., MARRADI A. (1996), *Intervista*: https://www.treccani.it/enciclopedia/intervista_%28Enciclopedia-delle-scienze-sociali%29/.

TSIOURAS I. (2020), *GDPR. Privacy Risk Management*, Youcanprint, Lecce.

TUCKER C. E. (2014), *Social networks, personalized advertising, and privacy controls*, Journal of Marketing Research, 51(5), 546-562.

USEEM M. (1996), *Investor Capitalism: How Money Managers are Changing the Face of Corporate America*, New York, Basic Books.

VAALAND T., HEIDE M., GRONHAUG K. (2008), *Corporate social responsibility: Investigating theory and research in the marketing context*, European Journal of Marketing, 42(9/10), 927-953.

VARADARAJAN P., MENON A. (1988), *Cause-related marketing: To coalignment of marketing strategy and corporate philanthropy*, Journal of Marketing, 52, 58-74.

VERDE M. (2017), *Responsabilità sociale di impresa tra teoria e prassi. Il bilancio sociale come processo di costruzione di senso*, G. Giappichelli Editore, Torino.

VIDAL F. (2015), *Historical and Ethical Perspectives of Modern Neuroimaging*, in CLAUSEN J., LEVY N. (eds), *Handbook of Neuroethics*, Springer, Dordrecht.

WADDOCK S. A., GRAVES S. B. (1997), *The corporate social performance-financial performance link*, Strategic Management Journal, 18(4).

WALTON C. C. (1967), *Corporate social responsibilities*, Belmont, Wadsworth Publishing Company.

WARTICK S., COCHRAN P. (1985), *The evolution of the corporate social performance model*, Academy of Management Review, 10.

WATKINS S. G. (2013), *An Introduction to Information Security and ISO 27001:2013. A Pocket Guide*, Second Edition, IT Governance Publishing.

WERTHER W. B., CHANDLER D. (2010), *Strategic corporate social responsibility: Stakeholders in a global environment*, Sage Publications, Thousand Oaks.

WESTIN A. F. (1967), *Privacy and Freedom*, New York: Atheneum, First Edition.

WHITE T. B., NOVAK T. P., HOFFMAN D. L. (2014), *No strings attached: When giving it away versus making them pay reduces consumer information disclosure*, Journal of Interactive Marketing, 28(3), 184-195.

WHITE T. B., ZAHAY D. L., THORBJØRNSEN H., SHAVITT S. (2008), *Getting too personal: Reactance to highly personalized email solicitations*, Marketing Letters, 19(1), 39-50.

WOOD D. J. (1991), *Corporate social performance revisited*, Academy of Management Review, 16(4), 691-718.

WOOD D. J. (1991), *Social issues in management: Theory and research in corporate social performance*, Journal of Management, 17, 383–406.

WORKING PARTY ARTICLE 29*, Statement of the Working Party on current discussion in the Council regarding the EU General Data Protection Regulation*, *Main points for one-stop-shop and consistency mechanism for business and individuals*, 16 aprile 2014.

YELKIKALAN N., KÖSE C. (2012), *The effects of the financial crisis on corporate social responsibility*, International Journal of Business and Social Science, 3(3), 292-300.

YIN R.K. (1981), *The Case Study Crisis: Some Answers*, Administrative Science Quarterly, Vol. 26, No. 1, pp. 58-65.

YIN R.K. (1984), *Case Study Research: Design and Methods*, Beverly Hills, Calif, Sage Publications.

YOUTUBE, *Insights Talk – Parliamo di gestione della privacy con Giampiero Raschetti, di Banca Popolare di Sondrio*: https://www.youtube.com/watch?v=Kc3x3u5G_Fk.

ZAINAL Z. (2007), *Case study as a research method*, Jurnal Kemanusiaan, bil. 9.

ZAMBRANO V. (2019), *Il Comitato europeo per la protezione dati*, in CUFFARO V., D'ORAZIO R., RICCIUTO V. (a cura di), *I dati personali nel diritto europeo*, G. Giappichelli Editore, Torino.

ZORZI GALGANO N. (2019), *Persona e mercato dei dati. Riflessione sul GDPR,* Cedam, Padova.

ZYGLIDOPOULOS S. C. (2002), *The social and environmental responsibilities of multinationals: evidence from the brent spar case*, Journal of Business Ethics, 36 (1-2).

# NOTE SULL'AUTORE

**Andrea Roberto Musolino**. Lombardo, classe 1993, è *doctoral researcher* in *Marketing* (SECS-P/08 – Economia e gestione delle imprese) presso il Dipartimento di Comunicazione e Ricerca Sociale della Sapienza Università di Roma. Socio corrispondente della *Società Italiana Marketing*, è autore di articoli scientifici e relatore di *conference papers* in ambito *marketing management*. Ha partecipato a scuole di metodologia della ricerca, seminari, convegni, conferenze, laboratori. I suoi interessi scientifici di ricerca s'incentrano nei seguenti ambiti: *privacy and data protection*, *agri-food marketing*, *brand management*, *sustainability, corporate social responsibility*. Ha maturato esperienza lavorativa in qualità di *communication assistant* al Ministero delle politiche agricole, alimentari e forestali e come *business accountant* in uno studio commercialista.

**Contatti**

+39 346 519 7717

andrearoberto.musolino@uniroma1.it

andrearoberto.musolino@gmail.com

LinkedIn: andrearobertomusolino