

# Indice

- p. 11 Presentazione di Domitilla Benigni
- 13 Prefazione di Filomena de Santis
- 17 Introduzione
  
- 25 Capitolo 1  
*Opportunità e rischi della trasformazione digitale*
  
- 33 Capitolo 2  
*Il GDPR*
  - 2.1. Timeline del GDPR, 33
  - 2.2. L'accountability, 35
  - 2.3. GDPR e sicurezza, 41
  - 2.4. Privacy by design e by default, 46
  - 2.5. La figura del DPO, 47
  
- 51 Capitolo 3  
*Il sistema di gestione privacy*
  - 3.1. Il Modello PDCA, 51
  - 3.2. Pianificazione, 53
  - 3.3. Audit, 54
  - 3.4. Il sistema di gestione per la privacy alla prova del Covid, 54
  
- 59 Capitolo 4  
*Compliance: un approccio per processi*
  - 4.1. L'avvio del progetto di compliance, 60
  - 4.2. Due possibili scenari, 61

- 4.3. La Gap Analysis, 64
  - 4.4. Il Framework PCF di APQC, 66
  - 4.5. Il Privacy Management Accountability Framework di Nymity, 68
  - 4.6. L'applicazione combinata dei due Framework, 68
  - 4.7. Il Framework Nazionale per la Cybersecurity e la Data Protection, 95
- p. 101 Capitolo 5
- La valutazione d'impatto privacy*
- 5.1. Considerazioni di contesto, 102
  - 5.2. Sicurezza e standard, 104
  - 5.3. Il processo DPIA, 107
  - 5.4. Le fasi del Processo DPIA, 109
- 137 Capitolo 6
- La data breach notification*
- 6.1. Definizione di data breach, 138
  - 6.2. Impatto nelle aziende, 143
- 151 Capitolo 7
- Cloud e privacy
- 7.1. Caratteristiche essenziali, 152
  - 7.2. Modelli di deployment e di servizio, 152
  - 7.3. La sicurezza dei dati nel Cloud, 156
  - 7.4. Il Cloud e la privacy: indicazioni del Garante, 157
  - 7.5. Il Cloud e gli standard, 160
- 161 Capitolo 8
- La formazione
- 8.1. Vantaggi dell'*e-learning*, 162
  - 8.2. Efficacia della formazione *e-learning*, 164
- 169 Allegato. Il testo del Regolamento (Ue) 2016/679
- 357 Bibliografia
- 363 Indice delle figure
- 365 Indice delle tabelle
- 367 Ringraziamenti

## Presentazione

È davvero con piacere, e anche con un pizzico di orgoglio, che il Gruppo Elettronica ha contribuito alla pubblicazione di questo volume, scritto da Massimo e da Flavia Montanile su un tema, come la privacy, che vede la nostra azienda da sempre molto attenta, fino a definirsi un'organizzazione *privacy oriented*.

Nel panorama della discussione attualissima sulla privacy, anche all'interno delle aziende, questo volume porta valore aggiunto per la serietà della ricerca originale intorno all'argomento. Ci inorgoglisce che Elettronica sia stata laboratorio concettuale e pratico delle migliori *practice* nei processi di trattamento dati, grazie anche all'esperto contributo di uno dei due autori, Massimo Montanile nel ruolo di Data Protection Officer della nostra azienda.

Al centro della nostra strategia aziendale ci sono sistemi per la sicurezza delle persone, che assumono un significato in più in un contesto operativo come quello della Difesa, in cui queste stesse persone hanno la titolarità della gestione di informazioni rilevanti per la sicurezza delle Istituzioni e della società civile.

Il libro offre alla riflessione dei lettori una *vision* della sicurezza e della privacy a livello di prassi operativa, attraverso l'individuazione di tutti quegli interventi auspicabili per un approccio sistemico al tema della sicurezza dei dati personali nel rispetto prioritario delle persone, e con particolare riferimento all'autodeterminazione informativa e alla non discriminazione. È questa la prova più ardua, ma anche più concreta di questo metodo di lavoro, verificato sul campo e raccontato dal libro che, a differenza dell'ampia letteratura sul tema, offre uno sguardo ai processi visti nella loro realizzazione pratica.

Domitilla Benigni

## Prefazione

L'arte della memoria ha radici in un passato molto remoto. Nel *De oratore* Cicerone ascrive al poeta Simonide di Ceo l'introduzione del concetto secondo cui la capacità di ricordare sia legata all'utilizzo, correlato ad un determinato ordine, di luoghi e di immagini cosicché "i luoghi fungano da tavolette per scrivere e le immagini da lettere con cui scrivere".

Le mie tavolette sono aule, laboratori, uffici, giardini della Facoltà di scienze matematiche, fisiche e naturali dell'Università degli Studi di Salerno, sita negli anni '80 in un territorio della Valle dell'Irno del quale i due piccoli centri di Baronissi e Lancusi reclamavano l'appartenenza. Le mie lettere sono studenti, docenti, amministrativi, della facoltà, ma soprattutto del corso di laurea in scienze dell'informazione cui afferivo: un microcosmo tranquillo, combattivo, altezoso, vanitoso, matto, contemplativo, premuroso e potrei continuare per molto ancora per dare spazio alle sensazioni ed alle emozioni che provavo e che, incontenibili, riaffiorano da tracce indelebili lungo le strade della vita.

In queste tavolette ritrovo Massimo Montanile, uno degli autori del libro per il quale ho l'onore di scrivere la prefazione. La freschezza della gioventù arrideva ad entrambi: Massimo studente di grande valenza, dedizione e sensibilità, io docente in carriera con l'ansia perenne della chiarezza espositiva nelle mie lezioni, entrambi particolarmente affascinati dai modelli di calcolo che catturassero la nozione di computabilità effettiva. Abbiamo fatto tanta strada insieme tra lezioni, esami, discussioni, pause caffè che, a partire dagli aspetti computazionali legati alla progettazione di algoritmi efficienti per problemi combinatoriali, hanno prodotto come risultato finale una validissima tesi su algoritmi di approssimazione per problemi NP-Completi. Essa, però, è solo un volto della nostra lunga collaborazione che ci ha consentito di scoprire molti

spazi delle interiorità che ci appartengono, primo fra tutti quello della famiglia, vissuta da entrambi come il riparo da ogni paura in cui il rispetto per le vite dei singoli regna padrone. Dal momento della laurea ad oggi, Massimo ha seguito un percorso ricco di successi nell'ambito dell'Information Technology e della Sicurezza delle Informazioni: ha maturato importanti esperienze in diverse aziende, pubblicato articoli e lavori sulla privacy in autorevoli riviste scientifiche, svolto quale docente corsi in master e scuole di perfezionamento. Insomma, se i presupposti di una brillante carriera c'erano tutti fin da quando ho conosciuto un giovanissimo studente di "grande valenza, dedizione e sensibilità", la pratica del lavoro, in un campo complesso e non sempre indulgente, ne ha dimostrato la veridicità. Con presunzione, mi riconosco il merito di aver saputo ammaliare con le sacre immagini della computabilità e della NP-completezza quel giovane studente ed annoverarlo tra i miei tesisti.

Con rammarico devo dire che la distanza geografica ed i ritmi frenetici del quotidiano non mi hanno consentito, al momento, di conoscere in persona Flavia Montanile della quale, tuttavia, ho potuto apprezzare l'attitudine alla multidisciplinarietà. Nonostante la giovane età, a partire da una formazione di tipo sanitario volta alla prevenzione, terapia e riabilitazione delle malattie neuropsichiatriche infantili, ha rivolto la sua attenzione e dato contributi anche al mondo dell'Information Technology. L'aggregazione delle sue competenze in due ambiti scientifici, apparentemente così lontani, è l'arma vincente che le riserverà un futuro pieno di stelle.

"Un modello per la sicurezza dei dati personali nell'era digitale" discute un argomento quanto mai attuale le cui radici affondano in un passato recente. La comunicazione è stato il fondamento dell'evoluzione umana e nel corso dei secoli la condivisione delle informazioni ha subito molti cambiamenti nelle forme in cui era realizzata: apparecchi sempre più sofisticati hanno preso il posto degli unici strumenti primordiali disponibili, voce e scrittura. Se la comunicazione per l'uomo è stata di fondamentale importanza, a maggior ragione lo è stata la comunicazione a distanza che vide la sua origine nel concetto di onda elettromagnetica introdotto da J.C. Maxwell nella seconda metà dell'800. La generazione e la rilevazione delle onde elettromagnetiche, dovuta ad H.R. Hertz trenta anni dopo, nonché gli innumerevoli esperimenti e risultati che seguirono consentirono a G. Marconi di aprire l'era delle telecomunicazioni nel 1896 e a R. Fessenden quella della telefonia mobile senza fili nel 1906. Le

dimensioni e il peso degli apparecchi cambiarono radicalmente con l'introduzione dei transistor nel 1948 preparando l'avvento dell'era digitale che vede un numero sempre crescente di persone connesse e di dispositivi collegati alla rete: una rivoluzione tecnica e di costume, dunque, fortemente caratterizzata da una navigazione in Internet, che possa supportare idee innovative, quali *smart city*, *self driving vehicles*, *Internet of Things* grazie a connessioni ultraveloci, a bassa latenza e ad alta densità. Se è evidente che le potenzialità di tale rivoluzione sono enormemente attraenti per tutte le categorie di utenti, è altrettanto evidente che è necessario un forte investimento in termini di lavoro per la definizione di standard di comunicazione, architetture di rete e normative. In una "grande rete" che sia in grado di collegare ogni cosa, è, infatti, imperativa l'esigenza di protocolli che definiscano quali caratteristiche debba rispettare la nuova generazione di trasmissione dati se si vuole evitare che la privacy delle persone venga messa a rischio e/o che ogni dispositivo connesso sia potenzialmente attaccabile per attività illecite. Il problema è ovvio, non altrettanto la sua soluzione a causa della grande quantità di interventi che bisogna effettuare affinché un'organizzazione possa adeguare i propri sistemi alle più attuali disposizioni nonostante la relativa intrinseca dinamicità. Particolarmente valido risulta, quindi, l'oggetto di questo libro, una guida operativa sulla privacy per la pianificazione dei singoli interventi di aggiornamento ed ottimizzazione dei sistemi preesistenti.

Mi concedo ancora poche parole per esprimere a Massimo e Flavia la mia gratitudine per avermi consentito di aggiungere un'altra tavoletta con tante belle lettere alla mia nutrita collezione.

*Filomena de Santis*

# Introduzione

La nostra storia, la nostra epoca, è stata ed è tuttora caratterizzata da una crescente interferenza tecnologica, sia in ambito lavorativo sia in quello personale. Troviamo, infatti, sempre più persone connesse, ed un crescente numero di *devices* collegati alla rete, tanto che già nell'anno 2010, il loro numero era maggiore della popolazione terrestre<sup>1</sup>. Sembra un'esagerazione, ma altro non è che la realtà. Citando Luciano Floridi, qualora nel 2010 fossero arrivati gli extraterrestri e avessero voluto studiare la comunicazione a livello quantitativo, avrebbero preso in considerazione le nostre tecnologie piuttosto che noi umani, in quanto la comunicazione sul pianeta Terra avviene per lo più tramite *devices*, i quali interloquiscono anche autonomamente tra loro, svincolandosi dal ruolo di funtori comunicativi in una visione umano-centrica. Questa simpatica e tagliente affermazione permette di aprire gli occhi su quanto spazio stia occupando questa evoluzione tecnologica, tanto da esser definita «la quarta rivoluzione»<sup>2</sup>. A proposito del concetto di spazio utilizzato, è sempre il

1. Dave Evans, *The Internet of Things How the Next Evolution of the Internet is Changing Everything*, White Paper CISCO, 4.2011, [https://www.cisco.com/c/dam/en\\_us/about/ac79/docs/innov/IoT\\_IBSG\\_0411FINAL.pdf](https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf).

2. Il termine Industry 4.0 è stato usato per la prima volta nell'anno 2011 dal professor Wolfgang Wahlster, direttore e CEO del Centro di ricerca tedesco per l'intelligenza artificiale, nel corso della cerimonia di apertura dell'Hannover Messe, la più importante fiera europea del mondo dell'industria e dell'automazione. Il termine sintetizza il cambio di paradigma contenuto nel progetto Industry 4.0 proposto dal gruppo di promotori Kommunikation der Forschungsunion Wirtschaft – Wissenschaft der Bundesregierung nelle sue "raccomandazioni d'azione" il 25 gennaio 2011 (cfr. Henning Kagermann, Wolf-dieter Lukas, Wolfgang Wahlster, *Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4. industriellen Revolution*, 1.4.2011 – <https://www.ingenieur.de/technik/fachbereiche/produktion/industrie-40-mit-internet-dinge-weg-4-industriellen-revolution/>). Il professor D. Zühlke, Scientific Director of Innovative Factory Systems (IFS) presso il German Research Center for Artificial Intelligence, ha definitivamente suggellato il nesso Industry

filosofo a descrivere per la prima volta l'infosfera, ovvero uno strato virtuale in cui sono contenuti tutti i dati che vengono prodotti da noi e dalle nostre tecnologie<sup>3</sup>. Dati che ormai sono fonte di ricchezza per le aziende contemporanee e, come ogni tesoro, sono soggetti ad essere scambiati, commerciati e trafugati. Ricchezze che necessitano di sicurezza e protezione, non solo fisica ma anche normativo-giuridica.

Quasi il 60% della popolazione mondiale è ora online, a luglio 2020 sono andate online per la prima volta 346 milioni di persone negli ultimi dodici mesi, e gli internauti hanno trascorso online mediamente nell'ultimo anno 6 ore e 42 minuti<sup>4</sup>. Se da un lato la tecnologia digitale sta portando enormi vantaggi economici e sociali per gran parte della popolazione, la mancanza di un quadro di *governance* globale della tecnologia rappresenta un rischio significativo.

Il quadro normativo nazionale ed europeo in tema di *cybersecurity* definisce in modo chiaro quali siano gli obblighi che le organizzazioni devono rispettare a fronte di un incidente di sicurezza, dettagliando cosa fare e quando farlo, lasciando tuttavia alle singole organizzazioni la scelta di come organizzare i propri processi interni per ottimizzare la gestione degli incidenti di sicurezza, nel rispetto della legge. La rivoluzione sta modificando ogni antica interpretazione, dalla comunicazione al commercio, trasformando di conseguenza anche gli attori e i loro ruoli. Si può per esempio pensare, in ambito di mercato, al *prosumer*, ovvero l'evoluzione del consumer classico in una figura più accattivante, la quale diventa oggi sempre più indispensabile. Si tratta praticamente della fusione tra *producer* e *consumer*, non solo in ambito linguistico, ma anche in un'ottica pratica. Come ripetuto più volte stiamo vivendo una rivoluzione e, in quanto tale, stiamo vivendo un'epoca di continue trasformazioni e mutazioni, radicate da tempo nella nostra società e in attesa di manifestarsi al momento più opportuno. L'idea del *prosumer* nasce per opera di Alvin Toffler, il quale descrive nel lontano 1980<sup>5</sup> la mutazione che nelle sue previsioni sarebbe avvenuta a carico del cliente passivo delle industrie. Egli teorizzava

4.0-quarta rivoluzione industriale quando, nel corso dell'Hannover Messe 2014, ha affermato che l'Industria 4.0 è la quarta rivoluzione industriale avviata e guidata dalla Germania.

3. *Infosfera: idee per capire il digitale*, lectio di Luciano Floridi, Teatro Franco Parenti, 20 giugno 2018, Milano.

4. We Are Social and Hootsuite, Global Digital 2020 reports, <https://wearesocial.com/digital-2020>.

5. A. Toffler, *The Third Wave*, Bantam Books (US), 1980.

che, in base all'evoluzione della tipologia di mercato che si andava sviluppando, anche il cliente avrebbe maturato una consapevolezza diversa e che, contemporaneamente al consumo, avrebbe prodotto dati ed informazioni utili sia al produttore e sia al futuro consumatore, diventando, parallelamente al suo *status* di consumatore, produttore. Prendendo spunto da questa affermazione, si può considerare il *single digital market*, spazio in cui maggiormente si concretizza quanto precedentemente teorizzato: il consumatore diventa produttore di informazioni utili ad altri consumatori e, contemporaneamente utili ai produttori che, sfruttando queste informazioni, riescono in modo sempre più preciso e contestuale ad affinare la produzione, per cucirla su misura per ogni tipo di cliente. Mercato che punta ad un'espansione sempre maggiore, tanto da necessitare di norme ben precise e regolamentate a livello centrale (europeo), per essere accessibile a tutti e in sicurezza. Da questo scenario complesso è evidente che serve ormai un approccio olistico se si vuole sperare di governare la sicurezza dei dati, in particolare di quelli personali.

Questione prepotentemente venuta alla ribalta in epoca di Covid-19 è poi quella relativa al bilanciamento dei diritti. Molti si pongono giustamente domande sul bilanciamento tra *privacy* e salute. In estrema sintesi i diritti di tutela dei dati personali recedono rispetto a quelli della salute pubblica e del singolo cittadino. Ciò è contemplato nell'impostazione del diritto europeo. Tuttavia, una volta stabilita la liceità di un trattamento alla luce di questa considerazione, resta in piedi l'obbligo del rispetto del GDPR che ovviamente non viene abolito... questo è un punto importante. Con ciò che ne consegue in termini di liceità dei trattamenti, informativa e misure di sicurezza da adottare.

Il legislatore nel 2016 aveva concesso due anni di tempo alle organizzazioni perché si adeguassero. Sappiamo che molti hanno sprecato questa opportunità. Oggi purtroppo non tutti sono in grado di mettere in piedi le misure di sicurezza necessarie per proteggere i delicati dati raccolti con questi trattamenti particolarmente invasivi ma necessari (georeferenziazione, rilevazione della temperatura corporea dei lavoratori all'accesso, ecc.). Come ha ricordato, riferendosi alle misure anticoronavirus, Antonello Soro, quando era ancora Garante *privacy* italiano<sup>6</sup>: «I diritti possono, in contesti emergenziali,

6. Il 29 luglio 2020 si è insediato l'attuale Collegio del Garante per la protezione dei dati personali, composto da quattro membri eletti dal Parlamento, i quali rimangono in carica per un mandato di sette

subire limitazioni anche incisive, ma queste devono essere proporzionali alle esigenze specifiche e temporalmente limitate»<sup>7</sup>.

Ma quali sono i fattori contro? Il principale fattore negativo deriva in realtà da un punto di forza della rivoluzione stessa: la sua dinamicità. Questa sua peculiarità la rende una forza in espansione pluridimensionale, trasversale e verticale, che invade ogni angolo più intimo e remoto, fino a mostrarsi sfacciata sulla prima pagina di un *webjournal*. Dinamicità associata a celerità rendono il nostro paese, ancorato a vecchie tradizioni, ben distante da quella che oggi è una realtà incontrovertibile, cioè l'essere noi già in piena "rivoluzione". Ne consegue che bisogna navigare sull'onda del cambiamento per non venirne travolti e lasciati indietro, come un relitto sul fondale marino, sfuggendo ad ogni tentazione neoluddista di opposizione all'innovazione. Concepire questo cambiamento come se fosse un fiume in piena ci permette di comprenderne la potenza e la profondità, e quanto queste trasformazioni mirino a sradicare antiche convinzioni e vecchi concetti per portare una linfa che da dentro rinnovi il modo di interpretare la sicurezza in ottica privacy. Dunque, ciò che possiamo definire uno dei fattori contro è sicuramente la lentezza dei processi burocratici che da sempre si identificano come una delle criticità del "Bel Paese", penalizzando ormai da tempo i cittadini, sempre più incapaci di soddisfare molti bisogni e necessità del singolo. Inadeguatezze rese ancor più evidenti con l'avanzare di proposte e richieste sempre più esigenti, sempre più tecnologiche, sempre più sicure... Insomma, si tratta di una vera e propria sfida, quella di spezzare il binomio ossimorico di lentezza e velocità, intimamente congiunte nella danza del progresso. Si teme che non siano state adottate sufficienti misure per contrastare il rischio *cyber* e che la comunità globale sia generalmente mal posizionata per affrontare le vulnerabilità che hanno accompagnato gli avanzamenti del XXI secolo. Se associamo questa debolezza all'esiguità del *budget* messo a disposizione per sostenere i cambiamenti in corso, riusciamo a prevedere quanto questo nuovo movimento possa suscitare sconforto nei più, e come tale sentimento possa tradursi facilmente in dissuasione. Quanto descritto appare articolato, poiché un adeguamento ed un

anni non rinnovabile. Il collegio è così composto: Pasquale Stanzone (presidente); Ginevra Cerrina Ferroni (vicepresidente); Agostino Ghiglia (componente); Guido Scorza (componente).

7. ANSA, *Soro, sì alle misure anticoronavirus ma si rispettino i diritti*, 17 marzo 2020, [http://www.ansa.it/sito/notizie/topnews/2020/03/17/soro-si-alle-misure-anticoronavirus-ma-si-rispettino-i-diritti\\_837282ce-a26d-465e-9128-c8e606453cfo.html](http://www.ansa.it/sito/notizie/topnews/2020/03/17/soro-si-alle-misure-anticoronavirus-ma-si-rispettino-i-diritti_837282ce-a26d-465e-9128-c8e606453cfo.html).

aggiornamento, a prescindere dall'ambito in cui avvengano, richiedono indubbiamente una modifica strutturale, strumentale e personale.

In particolare, un aspetto negativo inerente alla flessibilità necessaria per affrontare il cambiamento si riscontra nella cultura generale, che porta tuttora ad interpretare la sicurezza esclusivamente (o principalmente) da un punto di vista fisico, senza concepire l'essenza della tutela di qualcosa che non sia materiale come i dati personali, i quali vanno difesi dal *cybercrime*, sempre più diffuso come tipologia di crimine e fortemente temuto, poiché difficilmente contrastabile in un contesto di sistemi progettati *insecurity by design*. Bisogna integrare gli approcci al fine di poter prevenire, insistendo sulla responsabilizzazione e sulla consapevolezza della fragilità del materiale che circola, della potenza che un attacco può scatenare a carico del singolo o di molti (*cyber attack* a danno di PA, banche, ospedali...). Ad oggi infatti, con lo sviluppo delle tecnologie, sono comparsi nuovi tipi di crimini i quali possono danneggiare non solo l'ambito economico, ma arrecare danni anche alla sicurezza militare e nazionale.

Ora, quali i fattori pro?

Non possiamo soffermarci solo sugli aspetti negativi, altrimenti crederemo anche noi che questa rivoluzione sia un buco nero pronto ad inghiottirci per non espellerci più. Sono infatti già notevoli i miglioramenti apprezzabili ormai oggi, e che ci si auspica, in un futuro prossimo, siano sempre maggiori. Un fattore indubbiamente positivo è l'energia che tutto muove fisicamente ed interiormente. Ed è quindi una spinta energica di cui si ha bisogno per guidare la rivoluzione.

Spinta che può essere raccolta dalle nuove generazioni, dai «nativi digitali»<sup>8</sup>, ovvero da coloro i quali fin da piccoli sono stati abituati a dimesticarsi con strumentazioni intelligenti, tanto da aver assicurato ad esse un ruolo centrale anche nelle attività ludico-ricreative. Sebbene i tradizionali negozi di giocattoli vadano sempre più spopolandosi, si osserva una crescita esponenziale nella vendita di giochi interattivi, volti all'educazione e all'insegnamento in un contesto giocoso. Sono sempre questi bambini che crescendo spingono per un'integrazione del mondo reale con il mondo virtuale, poiché per loro

8. Marc Prensky, *Digital Natives, Digital Immigrants, On the Horizon* (MCB University Press, vol. 9 n. 5, October 2001).

questa è una condizione innata, semplice e concreta. Sarà proprio da loro che dovremo prendere spunto, poiché la condizione che sperimentano può essere estesa su larga scala, permettendo di integrare nei diversi ambiti la tecnologia con intenti migliorativi. Le generazioni di cui si parla si succedono rapidamente, diffondendo una consapevolezza generale della necessità di approcciarsi ed aprirsi a questa rivoluzione con gli opportuni provvedimenti normativi. Provvedimenti che non tardano ad arrivare: adottato nel 2016 e diventato operativo nel 2018, il GDPR<sup>9</sup> pone le basi per un corretto sviluppo ed utilizzo di tutte quelle informazioni che derivano dalle nuove modalità di interazione e di relazione. Il Garante<sup>10</sup> pertanto, conscio della dinamicità della situazione in materia di sicurezza, è in costante aggiornamento, fornendo continue indicazioni sulla corretta attuazione delle norme. La pervasività degli interventi che è necessario attuare per implementare un sistema di gestione in grado di garantire, nel tempo, la *compliance* di un'organizzazione al quadro normativo *privacy*<sup>11</sup> richiede un approccio che, a partire dai processi in essere, ne consenta l'adeguamento o la revisione, eventualmente introducendone di nuovi, ottimizzando l'efficacia e l'efficienza del sistema nel suo complesso.

La decisione di scrivere una guida operativa sulla *privacy* nasce dalla convinzione che una tale azione di adeguamento possa beneficiare di uno strumento metodologico in grado di supportare una visione olistica che consenta di pianificare i singoli interventi necessari, avendo però chiaro il quadro d'insieme. La guida propone dunque un modello teorico di implementazione di un sistema di gestione per la *privacy*, accompagnato da applicazioni pratiche di immediato utilizzo, con *template* e *tool* pronti all'uso e facilmente adattabili per qualsiasi specifica necessità.

9. General Data Protection Regulation, Regolamento generale sulla protezione dei dati, Regolamento (UE) 2016/679.

10. Il Garante per la protezione dei dati personali 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.lg. 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).

11. Il quadro normativo *privacy* è caratterizzato da una pluralità di fonti, non tutte collocate allo stesso livello gerarchico. Le più rilevanti, ai fini del presente lavoro, sono: il Regolamento generale sulla protezione dei dati (Regolamento UE) 2016/679; il d.lgs. n. 196/2003 (codice della *privacy*) e ss.mm.ii., tra cui il d.lgs. n. 101/2018; le disposizioni ed i provvedimenti dell'Autorità garante italiana per la protezione dei dati personali.

A vantaggio dell'aspetto didattico del lavoro si propongono anche *use-case* tratti da casi reali, utili per valutare il livello di apprendimento della materia, nell'intento di fornire un ulteriore contributo alla finalità anche didattica del testo. Gli scenari proposti e gli argomenti trattati sono tutti stati affrontati in prima persona dagli autori, nei numerosi progetti cui hanno avuto l'opportunità di partecipare, in qualità di DPO o di esperti di Data Protection, di consulenti tecnici o organizzativi, ma anche e soprattutto ispirati dai quesiti posti dagli studenti nel corso di lezioni universitarie o nell'ambito dei corsi di formazione aziendali tenuti.