PRIVACY E INNOVAZIONE

STUDI E RICERCHE SULLA PROTEZIONE
DEI DATI PERSONALI NELL'ERA DIGITALE

10

PRIVACY E INNOVAZIONE

STUDI E RICERCHE SULLA PROTEZIONE DEI DATI PERSONALI NELL'ERA DIGITALE

La collana "Privacy e Innovazione" ospita i risultati delle attività di studio e ricerca avviate o promosse dal Centro studi privacy e nuove tecnologie: monografie tematiche, raccolte di scritti, *paper*, che seguono l'evoluzione del tema della protezione dei dati personali in una prospettiva multidisciplinare (giuridica, tecnologica, politico–sociale) proponendo chiavi di lettura innovative. La Collana può raccogliere inoltre gli atti dei convegni organizzati dal Centro studi, gli interventi e i documenti presentati dai Soci in occasione della partecipazione, in qualità di relatori, a conferenze e convegni, nonché ogni ulteriore contributo ritenuto meritevole. In "Privacy e Innovazione" sono pubblicate opere di alto livello scientifico, anche in lingua straniera, per facilitarne la diffusione internazionale.
Il direttore approva le opere e le sottopone alla revisione paritaria con il sistema del "doppio cieco" (*double blind peer review*) nel rispetto dell'anonimato sia dell'autore, sia dei due revisori che sceglie: l'uno da un elenco deliberato dal comitato scientifico, l'altro dallo stesso comitato in funzione di revisore interno. I revisori rivestono o devono aver rivestito la qualifica di professore universitario di prima fascia nelle università italiane o una qualifica equivalente nelle università straniere.

Ciascun revisore formulerà una delle seguenti valutazioni:

— pubblicabile senza modifiche;
— pubblicabile previo apporto di modifiche;
— da rivedere in maniera sostanziale;
— da rigettare;

tenendo conto della: *a)* significatività del tema nell'ambito disciplinare prescelto e originalità dell'opera; *b)* rilevanza scientifica nel panorama nazionale e internazionale; *c)* attenzione adeguata alla dottrina e all'apparato critico; *d)* adeguato aggiornamento normativo e giurisprudenziale; *e)* rigore metodologico; *f)* proprietà di linguaggio e fluidità del testo; *g)* uniformità dei criteri redazionali. Nel caso di giudizio discordante fra i due revisori, la decisione finale sarà assunta dal direttore, salvo casi particolari in cui questi provveda a nominare tempestivamente un terzo revisore a cui rimettere la valutazione dell'elaborato. Le schede di valutazione verranno conservate. Il termine per la valutazione non deve superare i venti giorni, decorsi i quali il direttore della collana, in assenza di osservazioni negative, ritiene approvata la proposta. Sono escluse dalla valutazione gli atti di convegno, le opere dei membri del comitato scientifico e le opere collettive di provenienza accademica. Il direttore, su sua responsabilità, può decidere di non assoggettare a revisione scritti pubblicati su invito o comunque di autori di particolare prestigio.

Classificazione Decimale Dewey:

342.40858 (23.) TUTELA DELLA RISERVATEZZA. EUROPA

Razmik Vardanian

La certificazione ai sensi del GDPR: uno strumento di *accountability* per lo sviluppo della cultura *data protection*

Prefazione di
Paolo Guarda
Giorgia Bincoletto

aracne

ISBN
979–12–218–2251–9

PRIMA EDIZIONE
ROMA 27 OTTOBRE 2025

Ai miei cari
che mi hanno sostenuto
in questo viaggio

Indice

13 Prefazione
Paolo Guarda, Giorgia Bincoletto

17 Introduzione

25 Capitolo I
La protezione dei dati personali nell'ordinamento europeo

1.1. Considerazioni preliminari, 25 – 1.2. Il *Risk Based Approach* nella disciplina sulla protezione dei dati personali, 32 – 1.3. I principi fondamentali per il trattamento di dati personali – il principio di accountability, 41 – 1.4. Gli obblighi di compliance di titolari e responsabili del trattamento, 50 – 1.4.1. Premessa, 50 – 1.4.2. *Privacy by design e privacy by default*, 52 – 1.4.3. Il registro delle attività di trattamento, 63 – 1.4.4. Valutazione d'impatto sulla protezione dei dati personali (*Data protection impact assessment*), 66 – 1.4.5. La sicurezza nel trattamento e la gestione dei *data breach*, 73 – 1.5. Certificazioni: definizioni, scopo e vantaggi, 82 – 1.6. Schemi di certificazione ISO in materia di sicurezza e protezione delle informazioni, 87 – 1.6.1. Cenni introduttivi, 87 – 1.6.2. Serie ISO/IEC 27000: *Information Security Management System (ISMS) Family of Standards*, 89 – 1.6.3. ISO/IEC 31700:2023: *Privacy by design for consumer goods and services*, 92 – 1.6.4. ISO/IEC 42001:2023: *Artificial intelligence – Management System*, 94 – 1.6.5. Normativa UNI 11697:2017: formazione e certificazione dei DPO, 95.

97 Capitolo II
Le certificazioni per la protezione dei dati personali ai sensi del Regolamento (Ue) 2016/679

2.1. Gli strumenti di autoregolazione volontaria nel GDPR: una breve panoramica sui codici di condotta, 97 – 2.2. Considerazioni preliminari sulle certificazioni per la protezione dei dati personali: definizioni, scopo e soggetti coinvolti, 109 – 2.3. La creazione di uno schema di certificazione ai sensi del GDPR, 119

– 2.3.1. I meccanismi di certificazione, 119 – 2.3.2. Ambito di applicazione e oggetto della certificazione (c.d. *target of evaluation*), 121 – 2.3.3. I criteri di certificazione e l'approvazione del meccanismo di certificazione, 125 – 2.3.4. La circolazione delle certificazioni nel Mercato Unico Europeo: la certificazione comune e il sigillo europeo per la protezione dei dati personali, 129 – 2.3.5. Gli Organismi di Certificazione: il loro ruolo nel processo di certificazione, 132 – 2.3.6. Procedimento di accreditamento degli OdC: requisiti e condizioni, 134 – 2.3.7. Opzione dualistica o monistica per l'organismo nazionale di accreditamento, 140 – 2.3.8. L'implementazione della disciplina GDPR sulle certificazioni all'interno degli Stati membri: l'esempio italiano, 142 – 2.3.9. Segue: i requisiti di accreditamento, 144 – 2.3.10. Segue: le valutazioni dell'EDPB sui requisiti aggiuntivi del GPDP, 147 – 2.4. Procedimento di certificazione, metodologia di verifica della conformità e monitoraggio successivo, 148 – 2.5. Ruolo e poteri delle autorità nazionali di controllo, 153 – 2.6. Effetti e vantaggi della certificazione ai sensi del GDPR, 159.

167 Capitolo III
Gli attuali schemi di certificazione idonei ai sensi del GDPR

3.1. Lo studio Tilburg per l'identificazione degli schemi di certificazione idonei ai sensi del GDPR, 167 – 3.2. Lo schema ISDP©10003:2020 per la protezione dei dati personali, 172 – 3.3. CNPD-GDPR *Certified Assurance Report Based Processing Activities* (GDPR-CARPA), 181 – 3.3.1. Caratteristiche del GDPR-CARPA, 181 – 3.3.2. L'intervento dell'EDPB: Opinion 1/2022 sullo schema di decisione dell'Autorità di supervisione del Lussemburgo riguardante i criteri di certificazione GDPR-CARPA, 192 – 3.4. European Privacy Seal (EuroPriSe©) per la certificazione dei trattamenti di dati personali svolti da responsabili del trattamento, 195 – 3.4.1. Caratteristiche di EuroPriSe©, 195 – 3.4.2. L'intervento dell'EDPB: Opinion 25/2022 sui criteri di certificazione EuroPriSe© per la certificazione dei trattamenti effettuati dai responsabili del trattamento, 207 – 3.4.3. Opinion 19/2024 EDPB e l'approvazione di EuroPriSe© come sigillo europeo per la protezione dei dati personali, 210 – 3.5. Europrivacy©: il Parere 28/2022 segna la nascita del primo sigillo europeo per la protezione dei dati, 212 – 3.6. La certificazione *EU Cloud Service Data Protection*, 219 – 3.7. La certificazione BC 5701, 228 – 3.7.1. Origini della certificazione BC 5701, 228– 3.7.2. Opinion 15/2023 e Opinion 27/2024 per l'approvazione dei criteri Brand Compliance su scala nazionale ed europea, 231 – 3.8. DSGVO-zt GmbH *certification criteria*, 234 – 3.9. La certificazione *IT-supported Processing of Personal Data* e il Parere 26/2024 dell'EDPB, 238 – 3.10. I nuovi schemi presentati nel 2025, 240.

243 Capitolo IV
Le certificazioni GDPR nella strategia digitale dell'Unione europea

4.1. Il futuro europeo definito dalla *European Data Strategy, Digital Services Package* e dalla regolazione dell'intelligenza artificiale, 243 – 4.2. *Digital Services Package*: come il mercato dei servizi digitali può impattare sulla protezione dei dati personali, 248 – 4.2.1. *Digital Services Act*, 248 – 4.2.2. *Digital Markets Act*, 253 – 4.3. La Strategia europea per i dati: come coniugare la libera circolazione dei dati con le certificazioni GDPR, 256 – 4.3.1. *Data Governance Act*, 256 – 4.3.2. *Data Act*, 261 – 4.4. Il Regolamento sull'intelligenza artificiale e la possibile applicazione delle certificazioni ai sensi del GDPR, 264.

275 Capitolo V
Le certificazioni privacy: cenni comparatistici

5.1. Le certificazioni privacy e data protection al di fuori dell'UE, 275 – 5.2. Regno Unito: Uk-GDPR e i primi schemi di certificazione approvati, 276 – 5.2.1. Cenni generali, 276 – 5.2.2. Age Check Certification Scheme (ACCS) e Age-Appropriate Design Certification Scheme (AADCS), 280 – 5.2.3. ICT Asset Recovery Standard 8.0 (ADISA), 282 – 5.2.4. UK GDPR Compliance Certification Scheme for the Provision of Training and Qualifications Services, 283 – 5.2.5. Lo schema LOCS:23 e considerazioni conclusive, 284 – 5.3. Canada: *Privacy by Design Certification Shield* del Privacy and Big Data Institute of Ryerson University, 286 – 5.4. Usa: le certificazioni privacy e il *Data Privacy Framework*, 291 – 5.5. Repubblica Popolare Cinese: PIPL e standard per il trasferimento transfrontaliero di informazioni personali, 301 – 5.6. Prospettive di armonizzazione normativa, 308.

311 Bibliografia

Prefazione

di Paolo Guarda[1] e Giorgia Bincoletto[2]

La disciplina europea in materia di protezione dei dati personali ha trovato, come noto, nel Regolamento (Ue) 2016/679 (Regolamento generale sulla protezione dei dati; di seguito: GDPR) il suo ultimo approdo. Questo non rappresenta certo una rivoluzione nel panorama europeo, ma si inserisce nel solco dei principi e delle scelte di fondo già operate vent'anni prima dal legislatore unionale con la Direttiva 95/46/CE. Alcuni concetti, però, possono essere rimarcati come novità. Tra tutti sicuramente la cosiddetta "*accountability*" (o "responsabilizzazione" nella – meno usata – versione italiana): la valutazione del contesto e la scelta delle soluzioni volte a mitigare i rischi sono completamente a carico di chi effettua e ha la responsabilità del trattamento dei dati (i.e. i titolari del trattamento).

L'*accountability* trova la sua prima espressione operativa nell'obbligo generale che impone di mettere in atto misure tecniche e organizzative adeguate a garantire l'applicazione della normativa e dimostrare la conformità di ogni attività di trattamento. L'attenzione rivolta ai titolari del trattamento e alla loro capacità di effettuare una corretta analisi dei rischi, tenendo conto di una serie di parametri che il Regolamento stesso indica, diventa l'aspetto fondante dell'approccio proattivo europeo, che viene poi arricchito dagli ulteriori principi chiave di "*data protection by design*" e "*data protection by default*". Il risultato di questa attività complessa deve corrispondere all'adozione di varie soluzioni, anche IT, volte a ridurre e, se possibile, eliminare

[1] Professore associato di Diritto privato comparato presso l'Università di Trento.
[2] Ricercatrice in Diritto privato comparato presso l'Università di Trento.

il rischio connesso al trattamento dei dati personali, fin dalla progettazione e per tutta la sua durata.

È in tale contesto che si colloca il nuovo – efficace – strumento di natura volontaria investigato da quest'Opera. Le certificazioni hanno il potenziale per diventare un ottimo e utile supporto al titolare del trattamento per la gestione della sicurezza e conformità del trattamento, sia nella fase di valutazione del rischio che in quella di mitigazione dello stesso. Le regole che ne governano il processo di ottenimento e ne garantiscono la trasparenza giocano un ruolo di primo piano, in quanto essenziali per garantire effettività e valore alla certificazione stessa.

L'opera esplora l'istituto all'interno della disciplina a protezione dei dati personali e analizza la sua operatività, facendo leva sulla comparazione giuridica e sull'approccio interdisciplinare di Law & Technology.

L'analisi comparata risulta essenziale per poter svolgere una critica a compasso allargato al fine anche di descriverne la concreta applicazione negli ordinamenti giuridici scrutinati e di comprendere il diverso approccio che i sistemi giuridici seguono nell'applicare l'istituto e di individuare, in alcuni casi, imitazioni o potenziali nuovi modelli. L'interdisciplinarità, poi, caratterizza l'intero lavoro sul presupposto che lo scenario applicativo possa essere correttamente compreso solo con l'apporto di altre scienze e saperi.

Vengono, inoltre, presentati standard internazionali da tempo utilizzati nel mercato e vari meccanismi di certificazione già approvati dalle autorità europee e disponibili per i titolari del trattamento. La loro descrizione ed analisi offre a chi legge un interessante spaccato degli strumenti disponibili sul mercato, delle loro peculiarità e dei loro aspetti critici da un punto di vista operativo.

La dottrina ha colpevolmente poco affrontato questo tema considerandolo a volte come troppo tecnico. Esso, invece, ha solo parzialmente mostrato le proprie potenzialità e siamo sicuri diverrà centrale nell'attività di adeguamento e conformità alla disciplina europea sui dati personali. Queste pagine hanno, dunque, il pregio di aver finalmente proposto agli operatori giuridici

un'analisi ricostruttiva e critica e presentano le potenzialità per dar vita ad un dibattito sul punto al fine di valorizzare in maniera adeguata gli strumenti di *accountability* e soprattutto di far crescere la sensibilità sulla corretta gestione dei dati personali e sull'importanza dell'adozione di idonee misure di sicurezza e di soluzioni proattive per la tutela dei diritti degli interessati.

Il lettore saprà, pertanto, far tesoro della lettura di quest'Opera comprendendo la corretta enfasi che occorre riconoscere all'argomento trattato.

Introduzione

La protezione dei dati personali è un tema di grande attualità e rilevanza, soprattutto alla luce dei recenti sviluppi sui servizi dell'economia digitale e sull'intelligenza artificiale. Questi settori offrono nuove possibilità di raccolta, analisi e utilizzo dei dati personali, ma pongono anche nuovi rischi per la tutela della privacy e dei diritti fondamentali delle persone.

Con il sorgere di queste recenti sfide, anche l'applicazione del Regolamento generale sulla protezione dei dati (GDPR) è stata influenzata, registrando soluzioni innovative per la gestione della privacy informazionale allo scopo di adattarsi alle nuove esigenze e garantire un equilibrio tra innovazione e riservatezza. Ciò è rilevabile anche dai numerosi interventi giurisprudenziali, pronunciati dalla Corte di Giustizia dell'Unione Europea, e di *soft law*, da parte dell'European Data Protection Board (EDPB) e dalle autorità garanti nazionali per la protezione dei dati, al fine assicurare che la rivoluzione tecnologica europea avesse la data protection in cima alla lista delle priorità.

A fronte di tale contesto, sta ultimamente emergendo un importante mezzo per assicurare la corretta implementazione delle misure a protezione dei dati personali, ossia i meccanismi di certificazione. Questi ultimi, pur essendo espressamente disciplinati nel Regolamento (EU) 2016/679, non hanno ricevuto la dovuta considerazione negli anni immediatamente successivi alla piena attuazione della normativa europea, trovandosi in una sorta di stasi. Col tempo, tanto la dottrina quanto le istituzioni europee, sospinte dalle iniziative delle organizzazioni private, hanno riscoperto questo strumento.

Il presente lavoro si prefigge come scopo quello di porre in essere un'attenta analisi del ruolo delle certificazioni per la protezione dei dati personali come meccanismo efficace di

accountability per la dimostrazione della conformità del trattamento certificato alle norme del GDPR. Tali strumenti, previsti dagli artt. 42 e 43 del Regolamento, permettono di attestare l'adeguatezza e l'efficacia delle misure tecniche ed organizzative adottate per prevenire i rischi per i diritti e le libertà delle persone fisiche derivanti dai trattamenti di dati personali. Tuttavia, la materia delle certificazioni si rivela complessa e articolata poiché i precetti del GDPR sono concepiti secondo formule aperte che, se da un lato ne assicurano la flessibilità, dall'altro pongono significative sfide implementative. Per questo motivo, si rende necessario un approfondimento dei principi della protezione dei dati, attraverso un'indagine sistematica che ne segua le ramificazioni tra le diverse disposizioni presenti nell'articolato del Regolamento.

L'obiettivo della trattazione è quello di presentare un quadro ricostruttivo completo che possa risultare utile per la comprensione dello strumento certificativo non solo sul piano teorico ma anche in quello applicativo. Si intende, quindi, esaminare le caratteristiche generali delle certificazioni, i requisiti per il loro rilascio, le modalità di verifica e controllo, i benefici e i limiti, nonché gli schemi attualmente esistenti e le prospettive future per il loro sviluppo in relazione alla strategia europea digitale.

A fronte della rilevanza che la tutela dei dati personali ha assunto anche a livello internazionale, si è reso essenziale offrire una trattazione comparata di altri ordinamenti giuridici che dispongono di meccanismi di certificazione relativi alla privacy. Tale studio mira a individuare similitudini o possibili modelli di confronto rispetto a quanto sancito dalla legislazione europea.

La redazione del presente volume ha comportato l'adesione ad un approccio pratico, che non si limitasse a esaminare la normativa vigente, ma che tenesse conto anche delle linee guida e delle raccomandazioni emanate dall'EDPB, di vari contributi scientifici e divulgativi che illustrassero le modalità concrete di applicazione del GDPR, nonché della documentazione relativa ai vari meccanismi di certificazione analizzati, ove disponibili e pubblicati dai titolari degli schemi. In questo modo si è cercato di fornire una visione d'insieme delle principali caratteristiche e

dei vantaggi e svantaggi di ciascun sistema di certificazione, evidenziando le criticità sollevate e le opportunità per il miglioramento.

La struttura di questo volume si sviluppa come segue.

Considerando le complessità dei meccanismi di certificazione, nel primo capitolo si approfondiranno gli adempimenti e le principali garanzie che devono essere attuate in esecuzione dell'art. 5, par. 2 GDPR. Il Regolamento, infatti, introduce un impianto normativo per la protezione dei dati personali basato sul rispetto del principio di *accountability* e sulla tutela dei diritti fondamentali dell'interessato. Al suo interno, trovano collocazione le misure organizzative e documentali atte a garantire l'osservanza della disciplina. La nomina di un responsabile della protezione dei dati, la gestione della sicurezza e dell'integrità di questi ultimi, la valutazione d'impatto sulla protezione dei dati e l'istituzione di un registro riepilogativo dei trattamenti rappresentano gli elementi cardine del modello organizzativo che ogni titolare o responsabile è tenuto ad adottare per un lecito trattamento. Rispetto a questi adempimenti, le certificazioni possono rivestire una funzione importante nel quadro della responsabilizzazione di tali soggetti, al fine di documentare e di rendere conto della correttezza delle misure tecniche ed organizzative adeguate.

Affinché la certificazione fornisca prove affidabili della conformità in termini di protezione dei dati, il GDPR ha opportunamente fissato delle norme dirette a regolare il procedimento di certificazione. Pertanto, nel secondo capitolo, si esamineranno i concetti e i requisiti necessari per l'istituzione, la creazione, l'approvazione e l'assegnazione degli schemi di certificazione, individuandone la portata e l'ambito applicativo sulla base degli artt. 42 e 43 GDPR. Proprio queste ultime caratteristiche rappresentano la criticità più importante della disciplina. Il Regolamento, tuttavia, è silente nel dettare le condizioni in base alle quali i criteri di certificazioni debbano essere sviluppati. Per colmare tale incertezza, è stato quindi indispensabile l'intervento dell'EDPB che ha delineato i principi fondamentali su cui i meccanismi devono basarsi. Inoltre, verranno esaminati i vantaggi e le

conseguenze non solo giuridiche, ma anche reputazionali derivanti dall'adesione ad un meccanismo di certificazione, sia per i titolari del trattamento che per gli interessati.

Dall'aspetto giuridico-normativo delineato nei primi capitoli, si passerà a quello pratico, rappresentato dagli esistenti meccanismi di certificazione che sono stati approvati ai sensi dell'art. 42 GDPR. Delle soluzioni menzionate si esamineranno le caratteristiche principali quali: il loro campo di applicazione, le funzionalità, i criteri di controllo e le modalità di verifica post-rilascio. La sfida più grande che affronterà il terzo capitolo sarà quella di reperire fonti attendibili che descrivano adeguatamente le caratteristiche delle certificazioni esaminate. Queste sono da rinvenire nella documentazione tecnica relativa ai criteri di certificazione pubblicati dai vari titolari degli schemi e nei pareri rilasciati dall'EDPB per l'approvazione dei criteri di certificazione da parte delle autorità nazionali competenti. Proprio questi ultimi, al fine di garantire la massima specificità e coerenza espositiva, sono stati trattati, generalmente, in modo disgiunto dall'analisi degli schemi di certificazione. Tale approccio ha permesso di valorizzare tanto l'architettura di ciascuno schema quando, di approfondire in modo puntuale il contributo critico e orientativo offerto dall'EDPB.

L'elaborato prosegue sottolineando l'importanza delle certificazioni per la protezione dei dati personali come strumento di *accountability*, di trasparenza e di fiducia nel mercato digitale, nonché come opportunità di sviluppo e innovazione per le imprese che operano nel settore dei servizi digitali e dell'intelligenza artificiale. Il quarto capitolo sarà quindi dedicato ai diversi punti di contatto tra le certificazioni ai sensi del GDPR e i nuovi interventi legislativi avanzati dalla Commissione europea dal 2020 ad oggi per affrontare la nuova rivoluzione digitale scaturente dalla *datafication*.

Il capitolo conclusivo sarà dedicato all'esame della soluzione certificativa in una prospettiva comparata. L'obiettivo è estendere l'analisi oltre i confini dell'Unione Europea per esaminare il funzionamento dei regimi di certificazione in diversi sistemi giuridici, con particolare attenzione al Regno Unito, al Canada,