UNIVERSITY OF TRENTO
Faculty of Law

lawtech

Trento Law and Technology

Research Group

Student Paper n. 91

LA CERTIFICAZIONE AI SENSI DEL GDPR: UNO STRUMENTO DI *ACCOUNTABILITY* PER LO SVILUPPO DELLA CULTURA *DATA PROTECTION*

RAZMIK VARDANIAN

About the author

Razmik Vardanian (razmikxvardanian@gmail.com) graduated in Law at University of Trento under the supervision of Prof. Paolo Guarda (September 2023).

The opinion stated in this paper and all possible errors are the Author's only.

KEY WORDS

Certification – Data protection – Privacy – Accountability – Co-regulation

Sull'autore

Razmik Vardanian (razmikxvardanian@gmail.com) ha conseguito la Laurea in Giurisprudenza presso l'Università di Trento con la supervisione del Prof. Paolo Guarda (Settembre 2023).

Le opinioni e gli eventuali errori contenuti sono ascrivibili esclusivamente all'autore.

PAROLE CHIAVE

Certificazioni – Protezione dei dati personali – Privacy – Accountability – Co-regolazione

THE CERTIFICATION ACCORDING TO THE GDPR: AN ACCOUNTABILITY TOOL FOR THE DEVELOPMENT OF DATA PROTECTION CULTURE

ABSTRACT

The protection of personal data is a highly topical and relevant issue, especially in light of recent developments in computational science and artificial intelligence. These sectors, in fact, offer new possibilities for the collection, analysis, and use of personal data, but also present new challenges and risks for the protection of privacy and fundamental rights of individuals. With the emergence of these new challenges, the application of the General Data Protection Regulation (GDPR) has also been influenced, leading to new solutions for managing informational privacy to adapt to new needs and ensure a balance between innovation and confidentiality. This is also reflected in numerous rulings of the Court of Justice of the European Union and regulatory interventions by the European Data Protection Board (EDPB) and national data protection authorities, all aimed at ensuring that the European technological revolution places data protection at the top of the priority list.

Considering this context, an important tool has recently emerged to ensure the correct implementation of data protection measures, namely certification mechanisms.

This paper aims to conduct a thorough analysis of the role of data protection certifications as an effective tool for accountability in demonstrating compliance with GDPR regulations. These tools, as provided in art. 42 and 43 of Regulation (EU) 2016/679, allow for the attestation of the adequacy and effectiveness of technical and organizational measures taken to prevent risks to the rights and freedoms of individuals arising from the processing of personal data.

Considering the complexities of certification mechanisms, will be examined in depth the obligations and primary guarantees that must be implemented in accordance with art. 6, par. 2 of the GDPR to lawfully conduct personal data processing. Furthermore, we will outline the organizational methodology that an organization must adopt to document and be accountable for its processing activities.

In the second chapter, will be considered the concepts and requirements necessary for the establishment, creation, approval and allocation of certification schemes, identifying their scope and applicability based on art. 42 and 43 of the GDPR. These characteristics represent the most significant challenge in the certification discipline. Indeed, the Regulation is silent on dictating the conditions under which certification criteria should be developed. Due to this uncertainty, the intervention of the EDPB has become necessary to identify the key features of certification criteria on which the mechanisms should be based. Nevertheless, some aspects of the certification process remain uncovered. Finally, the thesis will explore the legal, as well as reputational, advantages and consequences resulting from participation in a certification mechanism, both for data controllers and data subjects.

From the legal and regulatory aspects outlined in the earlier chapters, will be moved on to address the practical aspect, represented by the existing certification mechanisms that have been approved under art. 42 of the GDPR. Will be scrutinized the main features of these solutions, such as their target of evaluation, functionalities, control criteria, and post-issuance verification mechanisms, in order to understand their effectiveness in establishing an appropriate technical and organizational framework for ensuring the proper processing of personal data.

The paper continues by emphasizing the importance of certifications for the protection of personal data as a tool for accountability, transparency and trust in the digital market, as well as an opportunity for development and innovation for businesses operating in the digital services and artificial intelligence sectors. This examination will be conducted by observing the various points of contact between the certification mechanisms under the GDPR and the new legislative initiatives put forth by the European Commission from 2020 to date to address the new digital revolution stemming from datafication.

Furthermore, the analysis has been enriched by describing the regulatory framework of some non-European jurisdictions. This comparative analysis allows to understand the role that privacy or data protection certifications play in strengthening national regulations and the culture related to the data protection. The results obtained from this study have shown how the "alignment" with the European Union's regulations has influenced the legislation of the United Kingdom in providing for co-regulation mechanisms that facilitate the implementation of obligations prescribed by the relevant national data protection regulations (UK-GDPR). In the United States and Canada, on the other hand, the situation is different: privacy certifications represent an attempt at private self-regulation that, in the absence of any public oversight, is at a higher risk of being susceptible to market abuses.

Certifications under the GDPR are certainly not a cure-all for resolving all the challenges that may characterize personal data processing, especially in more complex scenarios. However, they can help lay a solid foundation for effectively designing the technical and organizational measures required to meet the accountability principle. Adherence to a certification mechanism, as well as a code of conduct, represents the best option for ensuring transparency and the security of personal data processing, potentially increasing the trust of stakeholders in digital services and new technologies.

LA CERTIFICAZIONE AI SENSI DEL GDPR: UNO STRUMENTO DI ACCOUNTABILITY PER LO SVILUPPO DELLA CULTURA DATA PROTECTION

ABSTRACT

La protezione dei dati personali è un tema di grande attualità e rilevanza, soprattutto alla luce dei recenti sviluppi della scienza computazionale e dell'intelligenza artificiale. Questi settori, infatti, offrono nuove possibilità di raccolta, analisi ed utilizzo dei dati personali, ma anche nuove sfide e rischi per la tutela della privacy e dei diritti fondamentali delle persone. Con il sorgere di queste nuove sfide, anche l'applicazione del Regolamento Generale sulla protezione dei Dati Personali (GDPR) è stata influenzata, registrando nuove soluzioni per la gestione della privacy informazionale allo scopo di adattarsi alle nuove esigenze e garantire un equilibrio tra innovazione e riservatezza. Ciò è registrato anche dai numerosi interventi giurisprudenziali, della Corte di Giustizia dell'Unione Europea, e regolamentari, 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, recentemente sta emergendo un importante strumento per assicurare la corretta implementazione delle misure a protezione dei dati personali, ossia i meccanismi di certificazione.

Il presente elaborato intende compiere un'attenta analisi del ruolo delle certificazioni per la protezione dei dati personali come strumento efficace di *accountability* per la dimostrazione della conformità del trattamento certificato alle norme del GDPR. Questi strumenti, previsti negli artt. 42 e 43 del Regolamento (UE) 2016/679, 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.

Nel considerare le complessità dei meccanismi di certificazione, inizialmente si approfondiranno gli adempimenti e le principali garanzie che devono essere attuate in esecuzione dell'art. 6, par. 2 GDPR al fine di svolgere lecitamente un trattamento di dati personali. Inoltre, si darà conto della metodologia organizzativa che un'organizzazione deve adottare al fine di documentare e rendere conto delle proprie attività di trattamento.

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 sulle certificazioni. Infatti, il Regolamento è silente nel dettare le condizioni in base ai quali i criteri di certificazioni debbano essere sviluppati. In ragione di tale incertezza si è reso necessario l'intervento dell'EDPB al fine di individuare le caratteristiche principali dei criteri di certificazione in base ai quali i meccanismi

dovessero essere fondati. Ciononostante, rimangono alcuni punti scoperti in relazione al processo di certificazione. Infine, la tesi andrà ad esaminare 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 tratteggiato nei primi capitoli, si passerà ad affrontare il piano pratico, rappresentato dagli esistenti meccanismi di certificazione che sono stati approvati ai sensi dell'art. 42 GDPR. Di queste soluzioni si esamineranno le caratteristiche principali quali, il loro campo di applicazione, le funzionalità, i criteri di controllo e i meccanismi di verifica post-rilascio, al fine di comprenderne l'efficacia per la predisposizione di un assetto tecnico e organizzativo adeguato ad assicurare un corretto trattamento di dati personali.

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. Questo approfondimento verrà compiuta osservando i diversi punti di contatto tra i meccanismi di certificazione 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*.

Infine, l'analisi è stata arricchita dalla descrizione del quadro normativo di alcuni ordinamenti extraeuropei. La comparazione, infatti, permette di comprendere che ruolo hanno le certificazioni privacy, o *data protection*, nel rafforzamento della disciplina nazionale e della cultura relativa alla protezione dei dati personali. I risultati ottenuti da questa indagine hanno permesso di constatare come la 'vicinanza' con l'ordinamento dell'Unione europea abbia influenzato la legislazione del Regno Unito nella previsione di meccanismi di co-regolamentazione che consentano un'implementazione agevole degli obblighi previsti dalla relativa disciplina nazionale sulla protezione dei dati personali (UK-GDPR). Negli Stati Uniti e in Canada, invece, la situazione è opposta: le certificazioni *privacy* rappresentano un tentativo di autoregolamentazione privata che però, in assenza di alcun controllo pubblico, rischia maggiormente di prestarsi ad abusi da parte del mercato.

Le certificazioni ai sensi del GDPR non sono certamente la panacea per la risoluzione di tutti le criticità che possono caratterizzare il trattamento dei dati personali, in particolar modo per gli scenari più complessi. Esse possono, però, aiutare a gettare delle valide fondamenta per progettare efficacemente le misure tecniche ed organizzative necessarie per soddisfare il principio di *accountability*. L'adesione ad un meccanismo di certificazione, così come ad un codice di condotta, rappresenta la migliore opzione per garantire la trasparenza e la sicurezza di un trattamento di dati personali, incrementando potenzialmente la fiducia degli interessati nei servizi digitali e nelle nuove tecnologie.

INDICE

INTRODUZIONE

"*Noi pensiamo di discutere soltanto di protezione dei dati, ma in realtà ci occupiamo del destino delle nostre società, del loro presente e soprattutto del loro futuro*".

Rodotà, *Privacy, libertà, dignità*

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

Con il sorgere di queste nuove sfide, anche l'applicazione del Regolamento generale sulla protezione dei dati (GDPR) è stata influenzata, registrando nuove soluzioni per la gestione della privacy informazionale allo scopo di adattarsi alle nuove esigenze e garantire un equilibrio tra innovazione e riservatezza. Ciò è registrato anche dai numerosi interventi giurisprudenziali, della Corte di Giustizia dell'Unione Europea, e regolamentari, 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.

Questo lavoro si prefigge 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 Regolamento generale sulla protezione dei dati. Questi strumenti, previsti negli artt. 42 e 43 del GDPR, 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 è complessa e articolata, in quanto le norme del GDPR non sono complete ed esaustive. Per questo motivo, è necessario approfondire la materia attraverso un'analisi omogenea delle disposizioni del regolamento, che tenga conto della frammentazione della materia nelle varie norme presenti nel suo articolato.

L'obbiettivo 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 dell'importanza che la tutela dei dati personali ha assunto anche a livello internazionale, si è reso necessario offrire anche una trattazione comparatistica volta alla ricerca di ordinamenti giuridici in cui vi fossero meccanismi di certificazioni relativi alla privacy che potessero avere similitudini o potessero essere comunque impiegato come modelli di confronto con quanto sancito dal GDPR.

Per redigere questa tesi, ho dovuto seguire 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, pubblicati dai titolari degli schemi. In questo modo ho 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 tesi si articola nel seguente modo.

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. 6, par. 2 GDPR. Il Regolamento, infatti, istituisce un quadro di conformità per la protezione dei dati personali basato sul rispetto del principio di *accountability* e sulla tutela dei diritti fondamentali dell'interessato. Questo quadro comprende principalmente le misure organizzative e documentali atte ad assicurare l'osservanza dei principi del Regolamento. La nomina di un responsabile del trattamento, la gestione della sicurezza e dell'integrità dei dati, la valutazione d'impatto sulla protezione dei dati e l'istituzione di un registro riepilogativo dei trattamenti, fanno ormai parte della metodologia organizzativa che ogni titolare del trattamento deve adottare al fine di compiere un lecito trattamento di dati personali. Rispetto a questi adempimenti, le certificazioni possono rivestire una funzione importante nel quadro della responsabilizzazione del titolare del trattamento, 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 che introducono delle prescrizioni dirette a regolare il procedimento di certificazioni. 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. Infatti, il Regolamento è silente nel dettare le condizioni in base alle quali i criteri di certificazioni debbano essere sviluppati. In ragione di tale incertezza si è reso necessario l'intervento dell'EDPB al fine di individuare le caratteristiche principali dei criteri di certificazione in base ai quali i meccanismi dovessero essere fondati. Inoltre, la tesi andrà ad esaminare 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 tratteggiato nei primi capitoli, si passerà a quello pratico, rappresentato dagli esistenti meccanismi di certificazione che sono stati approvati ai sensi dell'art. 42 GDPR. Di queste soluzioni si esamineranno le caratteristiche principali quali: il loro campo di applicazione, le funzionalità, i criteri di controllo e i meccanismi di verifica post-rilascio. La sfida più grande affrontata dal terzo capitolo è stata quella di reperire fonti attendibili che descrivessero adeguatamente le caratteristiche delle certificazioni esaminate. Questa sono state principalmente reperite 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.

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 alle esperienze del Regno Unito, del Canada e degli Stati Uniti. La comparazione, come anticipato, permette di comprendere che ruolo hanno le certificazioni privacy (o *data protection*) nel rafforzamento della disciplina nazionale e della cultura relativa alla protezione dei dati personali. I risultati ottenuti in questo capitolo hanno permesso di constatare come la 'vicinanza' con l'ordinamento dell'Unione europea abbia influenzato la legislazione del Regno Unito nella previsione di meccanismi di co-regolamentazione che consentano un'implementazione agevole degli obblighi previsti dalla relativa disciplina nazionale sulla protezione dei dati personali (UK-GDPR). Negli Stati Uniti e in Canada, invece, la situazione è parallelamente opposta: le certificazioni *privacy* rappresentano un tentativo di autoregolamentazione privata che però, in assenza di alcun controllo pubblico, rischia maggiormente di prestarsi ad abusi da parte del mercato.

Le conclusioni, infine, saranno dedicate a riassumere sinteticamente i risultati di questa tesi ed a sottolineare come le certificazioni ai sensi del GDPR rappresentino un'opportunità importante per i titolari e i responsabili del trattamento al fine di progettare efficacemente gli assetti tecnici ed organizzativi necessari a predisporre un'organizzazione conforme agli adempimenti richiesti per garantire la tutela dei dati personali dell'individuo.

CAPITOLO I - LA PROTEZIONE DEI DATI PERSONALI NELL'ORDINAMENTO EUROPEO

1 Considerazioni preliminari

Il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (in seguito, "Regolamento" o "GDPR") relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, ha rappresentato un punto di svolta nella disciplina europea. Pietra miliare nella regolazione e tutela della *privacy*, intesa quale diritto fondamentale di ogni individuo, ha cambiato il modo di concepire la tutela della sfera privata delle persone fisiche. Tradizionalmente, infatti, la privacy è sempre stata considerata come diritto *tout court* alla riservatezza, una garanzia ad essere lasciati soli, senza interferente o intrusioni di terzi nella propria vita privata (*right to be let alone*) [1]. Tale concezione, pur essendo ancora forte oggigiorno, è stata rivoluzionata dall'evoluzione dell'economia digitale e dal massiccio utilizzo di dati personali per realizzare modelli di *business;* rivoluzione che ha mutato il diritto alla riservatezza da prerogativa passiva (azionabile solo in caso di violazioni) a diritto positivo, inteso come diritto di disporre attivamente dei propri dati personali e, di conseguenza, di esercitare il proprio diritto all'autodeterminazione informativa.

Segnato da tali principi, il Regolamento (UE) 2016/679 costituisce la conseguenza della 'Terza stagione della riservatezza' [2], data dall'emergere dei dati quale elemento fondamentale nella costruzione di un'economia digitale, e cioè caratterizzata da sistemi di produzione e scambio realizzati con infrastrutture informatiche. Questa, in realtà, comprende tutte le diverse tecnologie, sia hardware che software, sia online che offline, che garantiscono uno scambio e un'elaborazione di dati informatizzati: dai sistemi cloud al mobile, dall'Internet of Things ai Big Data, dai social network ai sistemi di realtà virtuale. Il fenomeno è ormai esploso da diversi anni, determinando sempre una maggiore integrazione e ibridazione tra il digitale e l'economia tradizionale, i cui processi produttivi vengono trasformati e ottimizzati dalla tecnologia digitale.

Considerata, quindi, la necessità di processare immense quantità di dati per costruire sistemi economici digitali, il rischio principale è quello per cui le economie liberali possano sfruttare arbitrariamente e ingiustificatamente i dati personali dei singoli, causandogli indelebili pregiudizi non solo alle loro libertà morali e personali.

Queste sono le problematiche che il GDPR intende prevenire. In particolare, esso si innesta nella valorizzazione europea della privacy operata dall'articolo 8, paragrafo 1 della CDFUE [3] e dall'art. 16, paragrafo 1, del TFUE, riconoscendo, quale principio

[1] Questa la prima ricostruzione dottrinale della nozione di privacy grazie all'intuizione dei due giuristi americani, Louis Brandeis e Samuel Warren. In tale accezione il termine *privacy* coincide in sostanza con la pretesa di ciascun soggetto ad impedire le altrui ingerenze nelle proprie vicende personali. Questa impostazione resta sostanzialmente immutata sino all'affermarsi della società digitale. Cfr. F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, Torino, 2016, 43-56.

[2] Come sottolineato da V. FRANCESCHELLI, *Premesse,* in E. TOSI (a cura di), *Privacy digitale: riservatezza e protezione dei dati personali tra* GDPR *e nuovo Codice Privacy,* Milano, 2019, XXXVII.

[3] Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adattata il 12 dicembre 2007 a Strasburgo, che, ai sensi dell'art. 6 TUE, ha lo stesso valore giuridico dei trattati.

generale, che "*La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale*". Come predicato, il GDPR discende dagli sviluppi tecno-economici avvenuti durante il vigore della Direttiva 95/46/CE (c.d. 'Direttiva Madre') e parallela disciplina nazionale di attuazione[4], la quale costituì il primo tentativo di bilanciare il diritto alla vita privata con il trattamento dei dati personali. Quest'ultima, però, aveva sempre a riguardo la riservatezza in sé considerata, mentre la tutela dei dati personali rappresentava solo un corollario applicativo della stessa. Con il Regolamento questo viene meno determinando l'avanzamento della privacy digitale a elemento centrale della regolazione europea, in virtù della globalizzazione e della digitalizzazione dell'economia globale.

Pertanto, l'evoluzione digitale e la frammentarietà della disciplina nazionale degli stati membri, a seguito del tentativo di armonizzazione della Direttiva Madre, hanno portato alla necessaria adozione di una disciplina regolamentare che garantisse uniformità all'interno del territorio dell'Unione, in ragione del considerevole aumento della circolazione transfrontaliera dei dati all'interno dei Paesi membri dell'Unione. Da questo punto di vista, si evidenza come il GDPR costituisca indice di attuazione del *Digital Single Market*[5], cioè nella strategia adottata dalla Commissione europea dal 2015 diretta a incentivare le attività digitali fra gli attori pubblici e privati, nonché a promuovere l'Unione europea alla testa dell'economia digitale globale[6]. Gli obiettivi principali dichiarati nella Strategia sono: sviluppare il commercio elettronico, modernizzare le leggi europee sul copyright, aggiornare la normativa sulle telecomunicazioni, rafforzare i presidi sulla *cybersecurity*, favorire il *free flow* di informazioni, migliorare le condizioni di connessione, adattare l'*e-privacy* al nuovo contesto e favorire lo sviluppo imprenditoriale digitale e le skills digitali dei lavoratori[7].

[4] 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. La Direttiva Madre era stata adottata con lo specifico scopo di armonizzare le norme in materia di protezione dei dati personali al fine di garantire un flusso libero dei dati e promuovere un elevato livello di tutela dei diritti fondamentali dei cittadini. La Direttiva è stata recepita in Italia, in primo luogo con la legge 31 dicembre 1996 n. 675 e successivamente, a conseguenza del crescente sviluppo della legislazione in tema, la disciplina in tema di protezione dei dati personali è stata organicamente interita all'interno del d.lgs. 196/2003 (c.d. codice privacy).

[5] Il Mercato Unico digitale, come espressione del pilastro del mercato unico dell'Unione europea, è formato, al pari di quest'ultimo, da quattro libertà fondamentali: la libera circolazione di merci, servizi, capitali e persone. Oggi, tuttavia, bisogna prendere atto che questi elementi, anche se rapportati al digitale, non sono rappresentativi della situazione economica contemporanea, tale per cui è necessario includere, nel quadro dei diritti fondamentali del mercato unico dell'Unione europea anche la libera circolazione dei dati.

[6] V. COMMISSIONE EUROPEA, *COM/2015/192, "Comunicazione della Commissione al Parlamento europeo e al Comitato delle regioni, Strategia per il mercato unico digitale in Europa*", 2015.

[7] Come evidenziato da E. PEDILARCO, *Il mercato unico digitale per l'integrazione europea. La prospettiva del FinTech*, in *MediaLaws*, n. 3, 2018, in Rete: *https://www.medialaws.eu/il-mercato-unico-digitale-per-lintegrazione-europea-la-prospettiva-del-fintech/*, il segno distintivo di cambiamento di strategia dalla precedente (concernente il commercio elettronico) e la nuova (appunto il mercato unico digitale) è rappresentato dalla Risoluzione 2014/2973(RSP) del Parlamento europeo del 27 novembre 2014 sul sostegno ai diritti dei consumatori nel mercato unico digitale. Egli sottolinea come "*Con tale risoluzione il Parlamento (i) invitava gli Stati membri e la Commissione a eliminare, attraverso sforzi volti ad attuare le regolamentazioni in vigore e a garantirne il rispetto nel quadro di una strategia globale, tutti gli ostacoli esistenti che si frappongono allo sviluppo del mercato unico digitale, garantendo nel contempo che tutte*

Come indicato dal Presidente della Commissione Jean-Claude Juncker, la strategia si baserà su tre pilastri fondamentali: "*1. migliorare l'accesso online ai beni e servizi in tutta Europa per i consumatori e le imprese; 2. Creare un contesto favorevole affinché le reti e i servizi digitali possano svilupparsi; 3. massimizzare il potenziale di crescita dell'economia digitale europea*". È quindi su questi presupposti che il GDPR si inserisce nella costruzione di un nuovo contesto economico-giuridico in cui la regolazione dei dati personali assume un ruolo di primo piano favorendone, da un lato, la tutela, in attuazione dell'art. 16 TFUE[8], e procedendo, dall'altro lato, all'organizzazione di un mercato economico-digitale in cui sia garantita la libera circolazione di tutti i dati[9].

Questa rivoluzione digitale non si è, però, arrestata alla protezione dei dati personali; anzi il GDPR ha posto le basi di partenza per realizzare una strategia legislativa di insieme che andasse a cogliere tutte le opportunità determinate dai progressi compiuti nei campi della robotica, intelligenza artificiale, blockchain [10], *cloud*

le misure siano valutate sotto il profilo dell'impatto, siano valide per le esigenze future e adeguate ai fini dell'era digitale; ritiene che tali sforzi debbano essere al centro degli sforzi profusi dall'Unione europea per generare crescita economica e occupazione e rafforzare la sua competitività e resilienza all'interno dell'economia globale e (ii) sottolineava che eventuali proposte legislative relative al mercato unico digitale avrebbero dovuto rispettare la Carta dei diritti fondamentali dell'Unione europea, in modo tale da garantire la piena tutela dei diritti in essa sanciti nel settore digitale".

[8] Cfr. Art. 16 del TFUE (ex articolo 286 del TCE): "*1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti. 3. Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea*".

[9] Come più compiutamente indicato dal considerando n. 13 del Reg. 2016/679: "*Per assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese, offra alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento e assicuri un controllo coerente del trattamento dei dati personali […]. Per il buon funzionamento del mercato interno è necessario che la libera circolazione dei dati personali all'interno dell'Unione non sia limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali. […]*".

[10] Cfr. PARLAMENTO EUROPEO, *INI/2018/2085, Relazione del Parlamento Europeo sulla blockchain: una politica commerciale lungimirante*, in Rete: *https://www.europarl.europa.eu/doceo/document/TA-8-2018-0528_IT.html*.

computing[11], *cybersecurity*, comunicazioni digitali e commercio elettronico[12]. Una volta disposte le norme fondamentali per realizzare una tutela omnicomprensiva dei dati personali, l'Unione europea è progressivamente intervenuta con nuove norme per stimolare l'economia dei dati, rimuovendo gli ostacoli principali alla libera elaborazione, circolazione e conservazione (anche transfrontaliera) dei dati industriali non personali e dei dati pubblici[13]. Ciò è altresì evidente se si considera la proficua attività legislativa della Commissione UE che, recentemente, ha adottato una serie di provvedimenti, tra proposte di regolamenti e direttive, connessi in modo intrinseco con la disciplina sulla protezione dei dati personali.

La proposta di Regolamento sull'intelligenza artificiale (*Artificial Intelligence Act*), il *Data Governance Act,* la proposta di Regolamento sulla regolazione dei dati (*Data Act*), *il Digital Services Act* e *Digital Market Act,* costituiscono la diretta conseguenza dell'intervento uniformante del GDPR e conseguenza della strada intrapresa verso una strategia europea in materia di dati (personali e non). In questo modo, l'Unione europea può divenire un modello di riferimento per una società che, grazie ai dati, dispone di strumenti per adottare decisioni migliori, a livello sia di imprese sia di settore pubblico.

Il perseguimento di questa proclamata sovranità digitale, da parte delle istituzioni dell'Unione, ha poi come diretta conseguenza anche una parziale estensione di alcuni diritti fondamentali centrali anche a soggetti terzi. È, infatti, evidente come la 'rivoluzione digitale europea'[14] impatti anche sui Paesi membri dello Spazio Economico Europeo, sugli stati terzi attualmente coinvolti nel processo di allargamento, nonché verso le nazioni extraeuropee che sono *partner* commerciali strategici dell'Unione. I risultati quali, ad esempio, il riconoscimento a 15 paesi extraeuropei di un livello di protezione dei dati personali adeguato a quello dell'UE, è una prova evidente della

[11] Cfr. COMMISSIONE EUROPEA, *COM/2012/0529, Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni: Sfruttare il potenziale del cloud computing in Europa*, 2012, in Rete: *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52012DC0529*; COMMISSIONE EUROPEA, *COM/2016/0178*, *Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni: Iniziativa europea per il cloud computing - costruire un'economia competitiva dei dati e della conoscenza in Europa*, 2016, in Rete: *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=COM:2016:178:FIN*.

[12] Cfr. CONSIGLIO DELL'UNIONE EUROPEA, *Press releases and statements 537/17, Remarks by President Donald Tusk after the Tallinn Digital Summit*, 2017, in Rete: *https://www.consilium.europa.eu/en/press/press-releases/2017/09/29/tusk-press-conference-tallinn/*.

[13] Cfr. CONSIGLIO DELL'UNIONE EUROPEA, *Press releases and statements 616/18*, *EU to strengthen sharing of public sector data - Council agrees its position*, 2018, in Rete: *https://www.consilium.europa.eu/en/press/press-releases/2018/11/07/eu-to-strengthen-sharing-of-public-sector-data-council-agrees-its-position/.*

[14] Ma anche le singole iniziative legislative, vedasi proprio il GDPR che nel definire, all'art. 3, l'ambito di applicazione territoriale, indica che il regolamento si applica anche "*[…] al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, […]*". Simile è la disposizione contenuta nell'art. 2 *Artificial Intelligentce Act* che prevede l'applicazione del regolamento "*ai fornitori che immettono sul mercato o mettono in servizio sistemi di IA nell'Unione, indipendentemente dal fatto che siano stabiliti nell'Unione o in un paese terzo*".

persuasività della diplomazia digitale europea[15]. È chiaro, quindi, che la gestione dei dati personali, oltre ad essere un fenomeno giuridico ed economico, è sempre più un fenomeno politico, capace di influenzare non solo il governo dei paesi membri, ma anche quello di stati terzi.

Osservando questi passaggi è facile intuire perché la visione futura dell'Unione sia concentrata sui dai, come stabilito, per ultimo, nella Comunicazione sulla Strategia europea dei dati, esposta dalla Commissione nel 2020, secondo cui: "*L'UE dovrebbe creare un contesto politico attraente, cosicché entro il 2030 la quota dell'UE dell'economia dei dati (dati conservati, elaborati e utilizzati proficuamente in Europa) corrisponda almeno al suo peso economico, non per imposizione ma per scelta. L'obiettivo è creare uno spazio unico europeo di dati – un autentico mercato unico di dati, aperto ai dati provenienti da tutto il mondo – nel quale sia i dati personali sia quelli non personali, compresi i dati commerciali sensibili, siano sicuri e le imprese abbiano facilmente accesso a una quantità pressoché infinita di dati industriali di elevata qualità, che stimolino la crescita e creino valore, riducendo nel contempo al minimo la nostra impronta di carbonio e ambientale. Dovrebbe trattarsi di uno spazio nel quale il diritto dell'UE possa essere applicato con efficacia e nel quale tutti i prodotti e i servizi basati sui dati siano conformi alle pertinenti normative del mercato unico dell'UE. Quest'ultima dovrebbe a tal fine combinare una legislazione e una governance idonee allo scopo per garantire la disponibilità dei dati, investendo in norme, strumenti e infrastrutture, come pure in competenze per la gestione dei dati. Un simile contesto favorevole, che offre incentivi e maggiori possibilità di scelta, comporterà un aumento dei dati conservati ed elaborati nell'UE*". Seguendo questa visione è evidente come l'UE intenda, quindi, inserirsi nello scacchiere politico-economico sui dati.

Nonostante le buone intenzioni della Commissione, rimane pur sempre problematico garantire un *enforcement* adeguato alla normativa europea sulla protezione dei dati, pur essendo la base di ogni strategia futura dell'Unione. In questo contesto, infatti, dove aumentano esponenzialmente non solo la qualità dei dati generati dai singoli individui, ma anche i rischi connesso ad un'economia digitale globale, è necessaria una metodologia per il trattamento dei dati personali che metta al primo posto gli interessi delle persone, in conformità ai valori e ai diritti fondamentali dell'Unione europea, rispetto agli interessi, legittimi, ma egoistici delle imprese.

Nel coordinamento di questi interessi, e rimanendo nel solco tracciato dalla Direttiva Madre, il GDPR costituisce una fitta trama di diritti e obblighi inerenti all'attività di trattamento dei dati personali. Da una parte ribadisce e introduce il novero dei diritti dell'interessato, ricavabili non sono in relazione ai principi che devono sovrintendere il trattamento dei dati personali (artt. 5, 6, 9), ma soprattutto nella specifica e completa previsione dei diritti dei quali è titolare l'interessato, quali il diritto di accesso, il diritto di rettifica, il diritto all'oblio, il diritto di limitazione del trattamento, il diritto alla portabilità dei dati, il diritto di opposizione al trattamento e il diritto a non essere sottoposto a decisioni automatizzate. Dall'altra, il Regolamento pone dei vincoli a carico del titolare e del responsabile del trattamento quanto alle modalità di trattamento e agli

[15] V. GPDP, *Trasferimento di dati personali all'estero*, in Rete: *https://www.garanteprivacy.it/temi/trasferimento-di-dati-all-estero* (ultima consultazione 22.08.2023) ove sono presenti i riferimenti alle decisioni di adeguatezza adottate dalla Commissione europea.

obblighi verso l'interessato, all'adozione di specifiche misure tecniche e organizzative volte a salvaguardare la sicurezza e l'integrità del trattamento, alla valutazione preventiva del rischio possibile e alla delineazione di una complessa documentazione diretta a guidare tali soggetti nell'implementazione dei meccanismi di *compliance* e, secondariamente, a garantire la trasparenza di quanto fatto nei confronti autorità pubbliche di controllo. Tutti questi ultimi elementi risultano infine specificazione e contenuto del più generale principio di *accountability,* inteso come obbligo del titolare del trattamento di rispettare tutti i diritti dell'interessato e i doveri a lui posti nell'attuazione del trattamento, di cui i principi all'articolo 5 costituiscono solo una punta dell'iceberg, e nella capacità contestuale di comprovare il rispetto dei medesimi.

In questo frangente le valutazioni del titolare del trattamento, nella predisposizione di un sistema di *governance* privacy del trattamento di dati, risultato del tutto autonome. Non vi è nessun intervento pubblico nella fase antecedente all'attuazione del trattamento (tranne per il meccanismo di consultazione preventiva di cui all'art. 36 GDPR). Eventualmente il titolare potrà essere guidato da elementi come codici di condotta o dalle condizioni per ottenere una certificazione, ma questi costituiscono solo mezzi che conducono il titolare nella scelta delle misure più idonee a garantire il rispetto dei diritti fondamentali e a prevenire situazioni di rischio connesse al trattamento.

2 Il Risk Based Approach nella disciplina sulla protezione dei dati personali

Si Con il progredire delle tecnologie e della tecnica, soprattutto nel settore imprenditoriale, si sono sviluppate molteplici situazioni di rischio prodotte dall'uomo che si sono aggiunte ai pericoli esistenti in natura. Sin dalla rivoluzione industriale, l'attribuzione di una responsabilità imprenditoriale per eventuali eventi dannosi creatosi in ragione dell'attività d'impresa esercitata, in quanto intrinsecamente rischiosa, ha determinato l'ampliamento delle responsabilità privata al fine di prevenire conseguenze dannose in capo ai singoli e di attribuire i costi della prevenzione del rischio ai soggetti con i requisiti economico-organizzativi necessari per raggiungere tal fine. In tal senso, la diretta attribuzione di questi rischi agli imprenditori ha fatto sorgere la necessità ideare un modello metodologico che permettesse di prevenire tali rischi, e pertanto, di ridurre le conseguenti responsabilità. La gestione del rischio, quindi, divenne un modello di *compliance* rispetto alle possibili conseguenze risarcitorie di eventi dannosi.

Allo stesso tempo, la gestione del rischio si è sviluppata anche nel campo pubblicistico. Sempre più spesso, infatti, attraverso la regolazione del rischio, il Legislatore è intervenuto disponendo quali attività dovessero essere regolamentate e il livello di *assesment* che sarebbe stato necessario predisporre per tutelare la società da nuovi elementi rischiosi, soprattutto nel campo della tutela dei consumatori e della concorrenza, della sicurezza alimenta, della medicina, dell'informatica e dell'ambiente[16]. Soprattutto in tema di nuove tecnologie, si è dunque intervenuti

[16] Il principio 'chi inquina paga' e le varie valutazioni di impatto sull'ambiente, disciplinate compiutamente, a livello comunitario, dalla direttiva 2001/42/CE, costituiscono i cardini della disciplina sulla sicurezza e tutela ambientale. Questa, genericamente, si caratterizza per l'analisi dei rischi ("impatto ambientale"), diretti o indiretti, che le attività produttive possono arrecare alla popolazione umana e

anticipando l'intervento regolatorio ad un momento in cui la conoscenza dell'oggetto da regolare è ancora incerta e lacunosa[17]. In questo modo, pertanto, la regolazione del rischio permette l'evoluzione della tecnica, in un contesto comunque protetto e procedimentalizzato, ma pur sempre flessibile, provvisorio e reversibile, in modo compatibile con i diritti ed interessi dei singoli.

Non da meno, anche il settore della privacy e della protezione dei dati personali sono caratterizzate da un approccio basato sul rischio, al punto che si può sostenere che il *risk-based approach* è parte integrante del GDPR. La gestione del rischio, tuttavia, non risulta una novità del Regolamento, in quanto questa era già ben definita anche sotto la Direttiva Madre, specialmente nella gestione della sicurezza[18] e controlli preliminari al trattamento[19]. Il regime giuridico applicabile al trattamento delle categorie particolari di dati può anche essere considerato come l'applicazione di un approccio basato sul rischio: obblighi rafforzati derivano da un trattamento considerato rischioso per le persone interessate[20].

Era pertanto evidente che, poiché il ritmo del cambiamento tecnologico superava le possibilità di adattamento tanto legislative, quanto imprenditoriali, un approccio basato sul rischio avrebbe dovuto migliorare la capacità dei responsabili della privacy e delle imprese di adottare un approccio strutturato e proporzionale, ma sicuro. Valutando le implicazioni sulla privacy dei dati di nuovi prodotti, servizi e altre attività, dal punto di vista di un eventuale impatto negativo sulle persone, l'obiettivo dovrebbe essere quello di ridurre la probabilità di un danno grave. L'approccio basato sul rischio va oltre la semplice conformità ai requisiti normativi. Essa va al cuore di ciò che le organizzazioni dei titolari e responsabili cercano di raggiungere, il modo in cui implementano i requisiti privacy sul campo e come dimostrano la conformità[21].

Nonostante ciò, Un approccio basato sul rischio dovrebbe basarsi in gran parte sulle disposizioni legislative esistenti ed emergenti che richiedono già una

---

salute umana; biodiversità; territorio, suolo, acqua, aria e clima; patrimonio culturale e paesaggio nonché l'interazione tra gli stessi. Cfr. M. PENNASILICO (a cura di), *Manuale di diritto civile dell'ambiente,* Napoli, 2014, 269-274.

[17] Cfr. P. SAVONA, *Il governo del rischio. Diritto dell'incertezza o diritto incerto?,* Napoli, 2013.

[18] Cfr. Direttiva 95/46/CE, art. 17: "*Sicurezza dei trattamenti. 1. Gli Stati membri dispongono che il responsabile del trattamento deve attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali. Tali misure devono garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere*".

[19] Cfr. Direttiva 95/46/CE art. 20, par.1: "*Gli Stati membri precisano i trattamenti che potenzialmente presentano rischi specifici per i diritti e le libertà delle persone e provvedono a che tali trattamenti siano esaminati prima della loro messa in opera".*

[20] Cfr. CENTRE FOR INFORMATION POLICY LEADERSHIP, *Project on Privacy Risk Framework and Risk-based Approach to Privacy,* 2014, in Rete: *https://www.informationpolicycentre.com/privacy-risk-management.html*.

[21] Cfr CENTRE FOR INFORMATION POLICY LEADERSHIP, *The Role Of Risk Management In Data Protection, in Project on Privacy Risk Framework and Risk-based Approach to Privacy,* 2014, in Rete: *https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_2-the_role_of_risk_management_in_data_protection-c.pdf.*

considerazione dei rischi per la privacy per gli individui. Questa nuova consapevolezza sul *risk based approach* può inoltre aiutare i legislatori a sistemare i loro problemi di interpretazione ed *enforcement* delle regole e per dare alle imprese una migliore idea di cosa aspettarsi dalla normativa (dunque maggiore certezza del diritto) e una più opportuna modalità per cautelarsi contro provvedimenti sanzionatori o interventi giurisdizionali.

Come efficacemente illustrato dal CIPL "*l'approccio e la metodologia della gestione del rischio mira principalmente a:*

1. *integrare le leggi e i regolamenti esistenti e facilitare l'applicazione dei principi e dei requisiti esistenti in materia di protezione dei dati;*
2. *contribuire ad attuare i requisiti giuridici e i principi sulla privacy esistenti in un contesto particolare, con maggiore flessibilità e agilità che è necessaria nella nuova era dell'informazione, tenendo conto dei rischi per le persone; e*
3. *migliorare l'attuazione di un'efficace protezione dei dati a beneficio di individui e organizzazioni che cercano una conformità più efficace, sistematica e dimostrabile"* [22]*.*

In questo contesto, anche se gli obblighi di *compliance* e *accountability* gravanti sul titolare del trattamento possono essere graduati sulla base del rischio, questo non li legittima a trascurare i diritti degli interessati o a evitare il rispetto degli obblighi legali derivanti dai principi generali del GDPR; questi, infatti, dovranno rimanere invariati indipendentemente dal rischio, di volta in volta, presentato dal trattamento[23].

Pertanto, essendo l'attenzione collocata sui rischi significativi per i dati personali delle persone, il Legislatore ha creato un contesto in cui il titolare del trattamento deve, in primo luogo, valutare se esista una significativa probabilità che una minaccia identificata possa portare a un danno riconosciuto, con un livello significativo di gravità e, in secondo luogo, deve gestire tale rischio. In questo ciclo di verifica è, pertanto, necessario individuare quali siano i possibili rischi di un trattamento, quali lesioni possono derivare da esso, quali sono gli interessi tutelati e le modalità per valutare probabilità e gravità de rischi, al fine di gestire il trattamento al meglio.

Partendo dall'analisi dei rischi del trattamento è, in via preliminare, necessario sottolineare che il titolare ha diversi strumenti a disposizione per valutare compiutamente le minacce che possono derivare dal trattamento: DPIA, sistemi di gestione della sicurezza informatica, registri e documentazione preliminare, ed altro. Questi strumenti, tuttavia, rischiano di porsi in un piano preliminare e astratto rispetto, poi, alla concreta esecuzione del trattamento. È per questo che è necessario, da parte del titolare, un approccio metodologico che si conformi non al trattamento in astratto, ma al trattamento in esecuzione. Il professionista deve, infatti, considerare l'intero ciclo del trattamento e l'elaborazione dei dati posta in essere da questo. Alcune minacce saranno visibili al momento della raccolta, ma alcune emergeranno in seguito, durante

[22] CENTRE FOR INFORMATION POLICY LEADERSHIP, *A Risk-based Approach to Privacy: Improving Effectiveness in Practice*, 2014, in Rete: *https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf*.

[23] Cfr. ARTICLE 29 DATA PROTECTION WORKING PARTY, *Statement on the role of a risk-based approach in data protection legal frameworks, 14/EN WP 218*, 2014, in Rete: *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf*.

l'uso o la divulgazione dei dati (situazione chiaramente patologica). È importante notare che le minacce possono anche cambiare durante il ciclo di vita delle informazioni, rendendo doveroso procedere ad una nuova verifica dei rischi e ad eventuale modifica della gestione degli stessi. Un esempio di rischi derivanti dal trattamento dei dati può essere: l'inesattezza dei dati; un ingiustificato o eccettivo trattamento (per finalità ulteriori rispetto a quelle originali o per fini inappropriati); l'uso di dati "sensibili"; la divulgazione non controllata; la perdita o il furto di dati; il trasferimento dei dati in paesi extra-UE. La vasta gamma di rischi, pertanto, dovrebbe determinarne, verso il titolare, una verifica costante e, soprattutto, relazionata al trattamento che si intende svolgere. Il contesto dev'essere il fattore determinante per valutare l'esistenza di una minaccia, il suo livello e il potenziale impatto lesivo e che rende, pertanto, flessibile l'impatto normativo degli obblighi gravanti sul titolare del trattamento[24].

Il rischio, tuttavia, altro non è che l'eventualità di subire un danno connessa a circostanze più o meno prevedibili[25]. Dunque, è necessario individuare quali sono i danni che potrebbero presentarsi, in relazione di una situazione rischiosa. In primo luogo, bisogna precisare che, nel contesto della protezione dei dati personali, per danno si intende ogni conseguenza negativa sia materiale che immateriale, economico, non economico o reputazionale per un individuo che può fluire dal trattamento dei dati personali[26]. Si estende a qualsiasi negazione dei diritti e delle libertà fondamentali. A fronte di tale definizione, quindi, un danno può essere:

1. una lesione tangibile per gli individui (lesione fisica, economiche, politiche, …);
2. un danno intangibile (intrusioni nella vita privata, discriminazioni, danni reputazionali, lesioni psico-emotive date dall'esposizione mediatica, …);
3. un danno sociale, spesso generato dalla sorveglianza di massa pubblica e/o privata (danno alle istituzioni democratiche, perdita della fiducia nella società, …).

I primi sono ben più probabili rispetto ai danni sociali. In relazione al trattamento di dati personali svolto, i danni tangibili e intangibili, possono essere meramente potenziali (un trattamento potrà probabilisticamente generare quell'effetto dannoso) o attuali (causalmente orientati a determinare quell'effetto).

In tema, poi, di modalità metodologiche, il titolare del trattamento deve sempre valutare l'esistenza di possibili eventi lesivi dai propri trattamenti in modo obiettivo, completo ed esaustivo, in modo da adottare tutte le misure tecniche ed organizzative adeguate a contenere il verificarsi degli stessi[27].

---

[24] D'altronde è lo stesso considerando n. 90 ad individuare che il titolare del trattamento, nella valutazione della probabilità e gravità del rischio debba tener conto della "*natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio*".

[25] Come definito dall'Enciclopedia Treccani, alla voce 'Rischio', in Rete: *https://www.treccani.it/enciclopedia/rischio#:~:text=Eventualit%C3%A0%20di%20subire%20un%20danno%20connessa%20a%20circostanze%20pi%C3%B9%20o%20meno%20prevedibili*.

[26] Cfr. R. GELLERT, *Understanding the notion of risk in the General Data Protection Regulation,* in *Computer Law & Security Review*, 2018, vol. 34, Issue 2, 279-288.

[27] D'altronde l'attività di trattamento dei dati personali è propriamente qualificabile come pericolosa, secondo i canoni di cui all'art. 2050, e pertanto, il titolare del trattamento è gravato da una posizione di garanzia nei confronti della società, dovendo adottare ogni cura e misura idonea ad impedire il verificarsi dell'evento dannoso a conseguenza dell'attività pericolosa (come anche specificato nell'art. 15 d.lgs. 196/2003 prima dell'abrogazione).

Minacce e lesioni, però, sono degli elementi asettici se privi di un collegamento. Una possibile lesione, infatti, potrà rappresentare un rischio solo allorché sia caratterizzata da una determinata gravità, in termini di lesività degli interessi degli individui, e da una certa probabilità. Ogni titolare del trattamento, pertanto, dovrebbe analizzare, in primo luogo, con quale probabilità un danno (anche fra quelli previamente elencati) potrebbe realizzarsi da un determinato rischio e quanto sarebbe grave l'evento lesivo ove effettivamente si concretizzasse. Quantificando e classificando i previ interrogativi si andrebbero a riscontrare tutti i rischi significativi che derivino dal trattamento, adottando poi tutte quelle misure tecniche ed organizzative volte a limitarlo [28] . Questo meccanismo di rilevazione dei rischi c.d. significativi rappresenterebbe un ottimo strumento per dare esecuzione al principio di *accountability,* quale primo strumento di carattere organizzativo che permette l'adozione di ogni misura di *compliance* successiva di carattere necessario, quale ad esempio una valutazione d'impatto sulla protezione dei dati personali. È chiaro che, in questo modo, dove si valuterà l'esistenza di un rischio significativo, potranno essere adottate tutte le misure ritenute idonee per proteggere gli interessati dai sopradescritti rischi. Nello specifico, questo eventualmente potrà comportare una modifica nella finalità del trattamento, nella gestione delle misure di sicurezza, nella mole di dati raccolti, o l'adozione di un nuovo o migliorato programma organizzativo per la privacy.

Da questa prospettiva, il *risk-based approach* permette di chiarire il presupposto di tutti quegli obblighi organizzativi sottesi alla regolamentazione. Il vantaggio principale, infatti, si riscontra nella successiva possibilità di modulare gli adempimenti necessari per assicurare un'adeguata protezione dei dati personali. Questo quadro migliorerebbe anche la capacità di gestione interna dei processi informativi, ma altresì l'attitudine delle organizzazioni di dimostrare a un terzo, compreso il regolatore, la loro *accountability*, consentendo loro di mostrare in modo specifico come e perché hanno raggiunto determinate decisioni in materia di trattamento dei dati. Sono certamente visibili, in questo modo, le conseguenze di un simile approccio con sistemi i sistemi di certificazione, attraverso la soddisfazione dei criteri in esse previsti, o con l'adesione ad un codice di condotta, soprattutto in tema di soddisfazione dei criteri in essi previsti.

In tema di vantaggi, poi, una gestione modulata del rischio, ove generalizzata fra le imprese, potrebbe altresì essere uno strumento utile per il Legislatore nel rafforzare la tutela della protezione dei dati personali. Attraverso una valutazione a matrice probabilità-gravità del rischio, il Legislatore, infatti potrebbe pensare di targettizzare la disciplina normativa per specifici settori o attività dove valuti possibile la probabilità di minacce o danni gravi; una simile gestione, inoltre, gli permetterebbe di evidenziare dove si aspetta che le imprese intervengano per gestire i rischi[29]; ciò gli permetterebbe comprendere se le imprese abbiano adottato misure di mitigazione del rischio appropriate in relazione alle capacità organizzative dell'ente e allo stato dell'arte. Infine,

[28] Cfr. CENTRE FOR INFORMATION POLICY LEADERSHIP, *A Risk-based Approach to Privacy: Improving Effective-ness in Practice*, *op.cit.*, 14-15. Il sopradescritto procedimento è descritto attraverso una matrice del rischio che permette di identificare la probabilità e gravità di rischi e, quindi, di individuare i rischi significativi da gestire.

[29] Cosa che attualmente avviene solamente su intervento delle autorità di controllo dei dati personali nazionali o dell'EDPB, spesso però successivamente all'emersione di controversie di rilevante entità.

un modello *risk based* potrebbe essere utilizzato anche dalle corti come strumento rimediale. Nel caso un individuo avesse subito un danno, questi strumenti potrebbero determinare come il danno si è verificato e i modi per evitare incidenti simili in futuro.

Pur essendo manifesti i vantaggi di questo modello, vi è una critica importante da evidenziare. Adottare al trattamento dei dati personali un approccio *risk based* non permette di eliminare in *toto* i rischi riscontrabili verso gli interessati. Questi potranno essere gestiti, mitigati e ridotti in termini di probabilità o gravità, ma una completa eliminazione degli stessi non è possibile. È per tale motivo che, soprattutto ai fini dell'esonero da sanzioni da parte dell'autorità di controllo o di condanne da parte dell'autorità giudiziaria, è necessario che il titolare sia in grado di dimostrare la bontà e la correttezza delle proprie scelte tecniche ed organizzative. Questo problema, ancorché rappresenti un grande limite al *risk based approach*, è comunque comune ad ogni possibile approccio adottabile nel campo della protezione dei dati personali. Infatti, soprattutto nel campo della *compliance* integrata[30] nelle imprese, qualora una certa attività sia connatura da una alea di rischio è oltremodo arduo che questa sia eliminata del tutto, ottenendo invece, nelle migliori delle ipotesi, un'attenuazione di suddette minacce, al fine, proprio, di evitare la responsabilità dell'organizzazione imprenditoriale.

Come espresso all'inizio del capitolo, l'importanza del *risk based approach* nella protezione dei dati personali è nettamente aumentata a partire dal GDPR, proprio perché il Regolamento ha cercato di farsi portatore di quei principi e proposte che nella precedente vigenza si erano consolidate nella prassi, pur se con diverse riserve inizialmente[31]. Il dibattito europeo, ha comunque portato ad un risultato apprezzabile dato che con il Regolamento si è riusciti a bilanciare un approccio basato sul rischio con un *right-base approach,* assicurando, pertanto, un "*livello minimo e non negoziabile di protezione per tutti gli individui*" [32] ed evitando invece che i diritti e libertà degli interessati fossero tralasciati da un *risk based approach* (per così dire) puro, che, invece, mette al centro i suddetti diritti solo quando eventuali lesioni siano sorte o siano suscettibili di sorgere[33].

Questo rapporto è evidente, per il *right based approach,* con i principi di cui all'art. 5 GDPR o l'elenco dei diritti degli interessati, i quali non possono mai essere derogati per ragioni attinenti all'assenza di rischi nel trattamento; mentre per l'elemento del *risk base approach* è proprio rinvenibile nell'art. 35, in tema di DPIA, il quale dispone come il

[30] Con ciò si intendono tutta la normativa nazionale ed europea fondata sul principio di *accountability* dell'ente stesso, rientrando, in tale ambito, non solo la protezione dei dati personali, ma anche la responsabilità amministrativa degli enti da reato (d.lgs. 231/2001), salute e sicurezza sui luoghi di lavoro (d.lgs. 81/2008), disciplina antiriciclaggio (d.lgs. 231/2007), anticorruzione (l. 190/2012), violazioni *antitrust* (l. 287/1990 e TFUE) e da ultimo la regolazione della crisi d'impresa (d.lgs. 14/2019).

[31] Cfr. CONSIGLIO DELL'UNIONE EUROPEA, *COD/2012/0011*, *Note on Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (GDPR)*, 2013.

[32] Come riconosciuto dal WP29, *Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS), OPINION 1/98, 1998, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp11_en.pdf.*

[33] Cfr. R. GELLERT, *Understanding the notion of risk in the General Data Protection Regulation*, in *Computer Law & Security Review*, 2018, vol. 34, issue 2, 279-288*;* ID*., Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative, in International Data Privacy Law,* 2015, vol. 5, Issue 1, 3-19.

titolare debba procedere ad una valutazione d'impatto sui dati personali, allorché un tipo di trattamento presenti un "*rischio elevato per i diritti e le libertà delle persone fisiche*". Rischio elevato che, quindi, può essere considerato corrispondente al precitato "rischio significativo", riscontrabile raffrontando gravità e probabilità delle varie situazioni rischiose. La possibilità di assumere una posizione versatile sulla gestione degli obblighi di *compliance* è poi prevista dal considerando n. 78, prevedendo che: "*la protezione dei diritti e delle libertà delle persone fisiche richiede l'adozione di misure tecniche e organizzative adeguate [al fine] di garantire il rispetto delle disposizioni del presente regolamento*". Questa frase riassume del tutto la logica *risk based* del GDPR, permettendo, senza trascurare diritti e principi minimi, che i rischi per i diritti e le libertà degli interessati influenzino direttamente il livello di *compliance* che dovrà mantenere il titolare del trattamento[34].

Alla luce dei principi esposti in precedenza è possibile interpretare il 'rischio elevato' come corrispondente al precitato 'rischio significativo', il quale sarà riscontrato ove il titolare ne valuti la significatività relazionando la gravità con la probabilità del verificarsi di un determinato danno, permettendo, di conseguenza, un approccio versatile nella gestione dei rischi.

3 I principi fondamentali per il trattamento di dati personali – il principio di *accountability*

Ai sensi dell'art. 5, par. 1, il trattamento deve essere informato ai seguenti principi:

- Liceità, correttezza e trasparenza: i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- Limitazione delle finalità: i dati sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo da non essere incompatibili con tali finalità;
- Minimizzazione dei dati: i dati devono essere adeguati, pertinenti, e limitati alle finalità per cui devono essere trattati;
- Esattezza: i dati personali sono esatti e se necessario aggiornati, devono essere adottate tutte le misure ragionevoli per cancellare i dati inesatti, rispetto alle finalità per cui sono trattati;
- Limitazione della conservazione: i dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- Integrità e riservatezza: i dati personali sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche, organizzative e adeguate a impedire trattamenti non autorizzati o illeciti, la perdita, la distruzione, o il danno accidentale.

Inoltre, *ex* art. 5, par. 2, il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo ('responsabilizzazione').

[34] Questo collegamento fra rischi riscontrati e *compliance* può essere ravvisato anche in relazione ai considerando n. 80, 81, 82.

Con l'evoluzione della normativa *data protection* dalla Direttiva Madre al GDPR, una novità importante è stata l'adozione del principio di *accountability*[35].

Il termine *accountability*, presente nel testo in lingua inglese del Regolamento, può essere tradotto come "responsabilità" o "prova di responsabilità". Esso è stato però trasposto, nel testo del Regolamento in lingua italiana, come "responsabilizzazione" e consisterebbe nell'obbligo di conformarsi (agli obblighi del Regolamento) e di dimostrare (la propria *compliance*)[36].

In ordine al suo significato, il WP29, nel parere 3/2010[37], ha evidenziato come *accountability* può essere tradotto in: responsabilità, affidabilità, assicurazione, obbligo di rendicontare, attuazione dei principi concernenti il trattamento dei dati personali.

Queste possibili traduzioni chiariscono alcuni aspetti dell'*accountability* e alcune conseguenze della stessa. Come precisato nel richiamato parere, "*l'architettura giuridica dei meccanismi di responsabilità prevedrebbe due livelli: il primo livello sarebbe costituito da un obbligo di base vincolante per tutti i responsabili del trattamento* (N.d.A. titolari del trattamento)*. Tale obbligo comprenderebbe due elementi: l'attuazione di misure e/o procedure, e la conservazione delle relative prove. Questo primo livello potrebbe essere integrato da disposizioni specifiche. Il secondo livello includerebbe sistemi di responsabilità di natura volontaria eccedenti le norme di legge minime, in relazione ai principi fondamentali di protezione dei dati (tali da fornire garanzie più elevate di quelle prescritte dalla normativa vigente) e/o in termini di modalità di attuazione o di garanzia dell'efficacia delle misure (norme di attuazione eccedenti il livello minimo)*"[38]. Il Regolamento, quindi, pone con forza l'accento sulla *accountability* di titolari e responsabili, dovendo, questi ultimi, adottare tutta una serie di atteggiamenti proattivi, volti, non solo a soddisfare le prescrizioni previste ma, soprattutto, a promuovere l'adozione di misure concrete ed effettive, in grado di adattarsi alla natura, portata, scopo e finalità del trattamento[39], e idonee a trasformare i principi del Regolamento in procedure pratiche formalizzate.

Questa posizione è altresì arricchita dall'obbligo del titolare del trattamento di dimostrare, non solo la reale adozione delle misure previste in applicazione del GDPR,

---

[35] Sull'*accountability* quale segno del cambio di paradigma presente nel regolamento 2016/679, v. C. BASUNTI, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali,* in *Contratto e impresa,* 2020, vol. 26 n. 2, 860-895.

[36] Il concetto di *accountability* è, in realtà, già presente dal 1980 nelle Linee guida della OECD (*Organisation for Economic Cooperation and Development*), in base alle quali: ''*A data controller should be accountable for complying with measures which give effect to the [material] principles stated above*''. Nell'ordinamento canadese il principio è menzionato nel *Personal Information Protection and Electronic Documents Act*.

[37] Cfr. WP29, *Parere 3/2010 sul principio di responsabilità, 62/10/IT WP 173,* 2010*,* in Rete: *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_it.pdf.*

[38] Cfr. *ivi,* punto 15.

[39] Come evidenziato da G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati,* in *Le Nuove Leggi Civili Commentate,* 2017, vol. 40, n. 2, 11: "*Occorre dunque una complessa attività di valutazione (tecnica, giuridica e organizzativa), un'analisi dei rischi e dei costi, una scelta sulle misure di sicurezza da adottare, l'istituzione di un presidio, l'emanazione di policy interne e quindi un'attività di monitoraggio continuo*".

ma anche l'efficacia e l'adeguatezza delle stesse [40]. Le prerogative del titolare, relazionate al *risk based approach,* determinano, quindi, in capo allo stesso, un particolare obbligo dimostrativo, risultando, per certi versi, come il rovescio della medaglia di un approccio teso a responsabilizzare quest'ultimo in relazione alla rischiosità afferente al trattamento svolto. Il Legislatore, infatti, in molti casi, come già anticipato, non detta più prescrizioni dettagliate, ma richiede invece al titolare del trattamento di effettuare le valutazioni sul caso specifico e conseguentemente di assumere le determinazioni relative all'adozione in concreto del principio sancito dalla norma.

In conclusione, come sempre evidenziato nel parere 3/2010 del WP29, due sono gli elementi principali su cui si concentrerebbe il principio dell'*accountability*:

1. la necessità che il titolare del trattamento adotti misure appropriate ed efficaci per attuare i principi di protezione dei dati;
2. la necessità di dimostrare, su richiesta, che sono state adottate misure appropriate ed efficaci. Pertanto, il titolare del trattamento deve fornire la prova di quanto esposto al punto precedente.

Come evidenziato in esordio del capitolo, il principio di *accountability* è espresso nell'art. 5 par. 2 del Regolamento. Questa, però, non è l'unica disposizione in cui è contenuto il principio, in quanto, esso è, in realtà, riportato all'interno di tutto il *corpus* del GDPR.

In primo luogo, può essere ritrovato nell'art. 24, considerato al pari dell'art. 5 la norma principale sul principio, il quale recita: "*Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché´ dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento*", evidenziando come il titolare debba compiere una valutazione di adeguatezza delle misure *ex ante* al trattamento e in una prospettiva prognostica agli sviluppi del trattamento. Al pari dell'art. 24, il principio è rinvenibile anche nell'art. 32, in tema di misure di sicurezza, nonché negli artt. 25 (*privacy by design & by default*), 30 (registro del trattamento), 31 (cooperazione con il Garante), 35 (procedura di *data breach*) e 36 (DPIA), nonché nell'adozione di modelli organizzativi. Questi ultimi rappresentano proprio gli strumenti che titolari (e responsabili) del trattamento devono adottare per garantire una corretta attuazione dei principi del Regolamento, dimostrando la propria *compliance* in caso di eventuali controlli dell'autorità di controllo o di terzi.

Cercando di trovare un *fil rouge* fra le disposizioni del regolamento, si può ritenere che il principio di *accountability* sia da richiamarsi ogni qual volta in cui al titolare siano

[40] Cfr. considerando n. 74: "*In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche*".

rimesse delle valutazioni in relazione al trattamento che viene effettuato[41]. Questa valutazione non è però ridotta solo alle scelte delle misure di *compliance* da adottare, ma ineriscono alla regolamentazione sostanziale del trattamento[42]. Ad esempio, nelle disposizioni di cui all'art. 12, in tema di informativa, rimettendo al titolare le scelte sui modi in cui concretamente fornire le informazioni[43]; all'art. 7, sul consenso, disponendo che "*qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali*"; all'art. 6 in relazione alla scelta della base giuridica del trattamento, e in particolare nella valutazione dell'applicabilità del legittimo interesse come presupposto di legittimità[44].

Particolare attenzione dev'essere poi prestata dal titolare nel trattamento delle categorie particolari di dati di cui all'art. 9 GDPR[45]. Data la sensibilità dei dati trattati è chiaramente necessaria l'adozione di misure tecniche ed organizzative supplementari rispetto ad un trattamento di dati personali 'comuni', atteso che il trattamento illecito di tali dati determinerebbe un sensibile pregiudizio in capo ai diritti e libertà degli interessati. Un esempio di applicazione del principio di *accountability* in relazione al trattamento di particolari categorie di dati è espresso nel parere formulato dal Garante per la protezione dei dati personali con il provvedimento n. 155 del 3 settembre 2020[46]. Il caso, in breve, riguarda una richiesta di accesso civico generalizzato formulata da un giornalista e rivolta alla Regione Valle d'Aosta; la richiesta, in particolare, aveva ad oggetto "*il rilascio di dati concernenti la distribuzione dei casi di Covid-19 registrati nella Regione Valle d'Aosta, suddivisi per comune, sesso, età, esito, domicilio, data della diagnosi di infezione, numero ed esiti dei tamponi eseguiti per paziente e concernenti*

[41] Ad esempio, in relazione all'applicazione del legittimo interesse come base giuridica del trattamento (art. 6, par. 1, lett. f) e anche in relazione alle valutazioni da effettuare in seguito al verificarsi di *data breach* (art. 33, par. 1).

[42] Cfr. G. FINOCCHIARO, *Il principio di accountability,* in *Giurisprudenza italiana,* 2019, vol. 171, fasc. 12, 2780-2781.

[43] Art. 12 GDPR: "*Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato*".

[44] Cfr. G. FINOCCHIARO, *Il principio di accountability*, *op. cit.* Sul punto, l'autrice sottolinea come "*al principio di accountability è necessario riferirsi per una lettura più piena e compiuta della base giuridica del legittimo interesse, che impone al titolare una comparazione fra il proprio interesse legittimo al trattamento e gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali*". Sul tema della liceità del trattamento per legittimo interesse e sulla responsabilità del titolare di individuare un equilibrio fra interessi contrapposti, v. EDPB, *Linea guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati (Vers. 2.0),* 2019.

[45] Il considerando n. 75 riconosce proprio come rischi per i diritti e libertà delle persone fisiche il trattamento di dati personali che "*che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza*".

[46] Cfr. GPDP, *Parere su istanza di accesso civico, registro dei provvedimenti n. 155 dd. 3 settembre 2020,* in Rete*: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9461036*.

numero, distribuzione per comune e data dei contatti telefonici della Centrale a ciò deputata con le persone prese in carico per infezione da Covid-19"[47]. La Regione ha accordato un accesso parziale, in ragione dell'"*interesse conoscitivo sotteso alla richiesta medesima*", fornendo i dati concernenti la distribuzione dei casi nella Regione, in forma aggregata, previa valutazione del pregiudizio alla protezione dei dati degli interessati nel caso di rilascio di tutte le informazioni. Tale soluzione è stata ritenuta conforme alla normativa in materia di protezione dei dati personali proprio alla luce del principio di responsabilizzazione, in quanto ha tenuto conto del contesto e del rischio di re-identificazione delle persone fisiche cui si riferivano i dati richiesti[48].

Nel Regolamento, poi, è posta particolare attenzione anche agli strumenti che possono dimostrare l'adempimento degli obblighi del titolare del trattamento, come individuati dagli artt. 24 e ss. Infatti, proprio il terzo paragrafo del medesimo articolo individua nell'adesione a un codice di condotta, conforme all'art. 40, o a un meccanismo di certificazione, approvato ai sensi dell'art. 42, due elementi utili a dimostrare l'attuazione del principio di *accountability*[49]*.* Questi strumenti non forniscono una presunzione legale, nemmeno relativa, sulla conformità al GDPR dell'attività di trattamento, lasciando, quindi, impregiudicati i compiti e i poteri delle autorità di controllo competenti. Piuttosto, codici di condotta e certificazioni evidenziano la proattività del titolare o responsabile del trattamento nella predisposizione di un assetto organizzativo e tecnico adeguato a garantire i diritti e libertà degli interessati, permettendo un'attenuazione dell'onere probatorio, ove costoro siano sottoposti a procedimenti giudiziari o ispettivi[50]. Una più approfondita trattazione dei vantaggi derivanti dall'ottenimento di una certificazione sarà comunque svolta nei capitoli successivi.

Tra le altre misure di cui il titolare o responsabile del trattamento potrebbe servirsi per dimostrare l'applicazione del principio di *accountability,* vi è quella di adottare *policy* che vadano a disciplinare, all'interno della loro organizzazione, i diversi aspetti del trattamento dei dati personali[51]. Un esempio di questi strumenti è espresso in "*Privacy*

[47] In quanto proprio ad oggetto dati sanitari, tale richiesta di accesso civico generalizzato è da considerarsi, per l'appunto, come trattamento di categorie particolari di dati ai sensi dell'art. 9 GDPR.

[48] Cfr. V. TEVERE, *Coronavirus: soggetti contagiati e profili di riservatezza - Garante Privacy, provvedimento n. 155/2020: è ammissibile un'istanza di accesso generalizzato ai dati concernenti la salute di soggetti contagiati da Covid-19?,* in *Altalex*, 2020, in Rete: *https://www.altalex.com/documents/news/2020/10/29/coronavirus-soggetti-contagiati-profili-riservatezza.*

[49] Questo, inoltre, lo si evince anche dal considerando n. 77: "*Gli orientamenti per la messa in atto di opportune misure e per dimostrare la conformità da parte del titolare del trattamento o dal responsabile del trattamento in particolare per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, e l'individuazione di migliori prassi per attenuare il rischio, potrebbero essere forniti in particolare mediante codici di condotta approvati, certificazioni approvate, linee guida fornite dal comitato o indicazioni fornite da un responsabile della protezione dei dati*".

[50] Cfr. D. POLETTI, M.C. CAUSARANO, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione,* in E. TOSI (a cura di), *Privacy digitale: riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy,* Milano, 2019, 379.

[51] Cfr. art. 24, par. 2: "*Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento*".

e Data Protection 2022", edito da IPSOAInPratica[52], nel quale sono state individuate, le principali *policy* interne utilizzate nella prassi:

- "*policy interna sul trattamento dei dati personali: contiene le principali istruzioni che i dipendenti e/o altri soggetti che operano nell'ambito dell'organizzazione del titolare sono chiamati a seguire nel trattamento dei dati personali;*
- *policy sull'esercizio dei diritti degli interessati: stabilisce i passaggi necessari a dare tempestivo seguito a eventuali richieste di esercizio dei propri diritti da parte degli interessati;*
- *policy per la gestione dei data breach: include regole e modalità pratiche di gestione di eventuali violazioni dei dati personali (data breach) che si dovessero verificare nell'ambito dei trattamenti effettuati dal titolare;*
- *policy sulle misure di sicurezza tecniche e organizzative: specifica le misure adottate dal titolare per minimizzare il rischio insito nei trattamenti svolti e garantirne la conformità alla normativa applicabile;*
- *policy sugli strumenti IT aziendali: specifica le regole relative all'utilizzo degli strumenti IT nell'ambito dell'organizzazione del titolare tra cui, ad esempio, la gestione dei dispositivi di memoria esterni e l'utilizzo di dispositivi personali ("BYOD" – bring your own device);*
- *policy sulla conservazione o data retention: consente al titolare di stabilire e documentare i diversi periodi di conservazione dei dati con riferimento a ciascuna finalità e di procedere alla cancellazione o anonimizzazione nelle tempistiche stabilite.*"

Gli autori evidenziano, altresì, che il livello di dettaglio di queste policy e la loro comprensibilità per i lavoratori coinvolti nell'organizzazione del trattamento è fondamentale per dimostrare il rispetto del principio di *accountability*. Se, infatti, le policy sono troppo generiche e non forniscono indicazioni dettagliate su come i dipendenti devono agire nel trattamento dei dati personali, le stesse potrebbero essere considerate inadeguate.

Infine, in relazione ai profili sanzionatori, va sottolineato che l'attuazione del principio di *accountability* (anche nella sua componente probatoria) possa rilevare ai fini dell'esclusione della responsabilità risarcitoria.

Ai sensi dell'art. 82 GDPR, chiunque abbia subito un danno patrimoniale o non patrimoniale connesso alla violazione del Regolamento ha il diritto di ottenerne il risarcimento dal titolare o dal responsabile del trattamento. Anche in questo caso, la lettera della norma indica una chiara inversione di tendenza rispetto alla disciplina previgente. In primo luogo, a differenza della disciplina ad esempio vigente in Italia, i soggetti legittimati passivi sono solo il titolare ed il responsabile del trattamento[53]. In secondo luogo, (elemento che più è rilevante ai fini della trattazione) il Regolamento esonera da responsabilità il titolare e il responsabile ove essi abbiano dato prova che

[52] Cfr. G. CORAGGIO (a cura di), *Privacy e Data protection 2022, IPSOAInPratica,* 2022, 26-28.

[53] La precisa formulazione consente di superare le incertezze interpretative poste dall'espressione utilizzata dalla Direttiva 95/46/CE, il cui art. 23 definisce genericamente il soggetto tenuto al risarcimento come "*responsabile del trattamento*".

l'evento dannoso non è in alcun modo a loro imputabile[54], nel senso di avere effettuato il trattamento in conformità del dettato normativo e, in riferimento al responsabile, nel rispetto dei compiti ad esso specificamente assegnati per via normativa o dal titolare[55]. In altre parole, la regola di condotta è distinta tra le diverse figure e modulata rispetto all'adempimento dei precisi obblighi indicati dal Regolamento, attenuando la *probatio diabolica* dell'estraneità della causa del danno alla propria sfera di rischio[56]. Infine, con l'art. 82, paragrafi 4 e 5, si stabilisce il principio di corresponsabilità, prevedendo che nel caso in cui vi siano uno o più titolari o responsabili implicati nel medesimo illecito trattamento, ogni soggetto è obbligato in solido a corrispondere l'intera somma dovuta a titolo di risarcimento, salva poi la possibilità di agire per ottenere il regresso sugli altri condebitori.

È evidente, pertanto, che più titolari e responsabili si doteranno di strumenti organizzativi che gli permettano di dimostrare la propria conformità alle disposizioni del GDPR, quali una certificazione, l'adesione a codici di condotta o, l'adozione di *policy* interne dettagliatamente documentate, quanto più sarà agevole dimostrare che questi abbiano adottato ogni misura utile a proteggere diritti e libertà degli interessati,

[54] Art. 82 par. 3 "*Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile*". Questo inciso lega la responsabilità di titolari e responsabili alla corretta attuazione, nel trattamento svolto, del principio di *accountability*.

[55] Cfr. il considerando n. 146: "*Il titolare del trattamento o il responsabile del trattamento dovrebbe risarcire i danni cagionati a una persona da un trattamento non conforme al presente regolamento ma dovrebbe essere esonerato da tale responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile. Il concetto di danno dovrebbe essere interpretato in senso lato alla luce della giurisprudenza della Corte di giustizia in modo tale da rispecchiare pienamente gli obiettivi del presente regolamento. Ciò non pregiudica le azioni di risarcimento di danni derivanti dalla violazione di altre norme del diritto dell'Unione o degli Stati membri. Un trattamento non conforme al presente regolamento comprende anche il trattamento non conforme agli atti delegati e agli atti di esecuzione adottati in conformità del presente regolamento e alle disposizioni del diritto degli Stati membri che specificano disposizioni del presente regolamento. Gli interessati dovrebbero ottenere pieno ed effettivo risarcimento per il danno subito. Qualora i titolari del trattamento o i responsabili del trattamento siano coinvolti nello stesso trattamento, ogni titolare del trattamento o responsabile del trattamento dovrebbe rispondere per la totalità del danno. Tuttavia, qualora essi siano riuniti negli stessi procedimenti giudiziari conformemente al diritto degli Stati membri, il risarcimento può essere ripartito in base alla responsabilità che ricade su ogni titolare del trattamento o responsabile del trattamento per il danno cagionato dal trattamento, a condizione che sia assicurato il pieno ed effettivo risarcimento dell'interessato che ha subito il danno. Il titolare del trattamento o il responsabile del trattamento che ha pagato l'intero risarcimento del danno può successivamente proporre un'azione di regresso contro altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento*".

[56] Nella disciplina italiana da responsabilità extracontrattuale, ad esempio, può essere inteso come mera prova del caso fortuito, della forza maggiore o di un elemento equivalente. Sul punto S. SICA, *La responsabilità civile per il trattamento illecito dei dati personali*, in A. MANTELERO, D. POLETTI (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa, 2018, 161-174. Nella giurisprudenza di legittimità italiana v. da ultimo Cass. civ., sez. VI, 5 settembre 2014, n. 18812, in *One LEGALE*, per cui "*i danni cagionati per effetto del trattamento dei dati personali in base all'art. 15 d.leg. 30 giugno 2003 n. 196, sono assoggettati alla disciplina di cui all'art. 2050 c.c., con la conseguenza che il danneggiato è tenuto solo a provare il danno e il nesso di causalità con l'attività di trattamento dei dati, mentre spetta al convenuto la prova di aver adottato tutte le misure idonee ad evitare il danno*".

andando sollevati, o quantomeno attenuati, da possibili responsabilità risarcitorie o sanzionatorie[57].

4 Gli obblighi di *compliance* di titolari e responsabili del trattamento

Se, come sottolineato, *l'accountability* è considerata più come un processo complesso piuttosto che, come un semplice risultato, questo approccio sottolinea maggiormente la necessità di analizzare in modo preventivo le tipologie di dati trattati, i rischi ad essi connessi e di scegliere le misure più adeguate da adottare in relazione alla struttura organizzativa del titolare (e responsabile) del trattamento, anche in relazione ai perduranti mutamenti del contesto tecnologico. La procedimentalizzazione di tale attività comporta, come necessaria conseguenza, il renderla documentabile al fine di "dar conto" delle proprie decisioni; ciò con il duplice scopo di attestare l'analisi degli elementi oggettivi presi in esame nel procedimento valutativo effettuato e di rendere tale articolata attività conoscibile e verificabile in caso di controllo esterno[58].

Per tali ragioni, è necessario interrogarsi sulle modalità concrete con cui il titolare possa "*garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al […] Regolamento".* Il GDPR accentua specifico approfondimento sia alle misure tecniche utilizzabili, ma soprattutto agli strumenti organizzativi implementabili dal titolare del trattamento. L'interessamento verso entrambi i fronti è da ricondurre al fatto che le tecniche e gli strumenti per assicurare la sicurezza del trattamento possono costantemente mutare, rendendo impossibile creare una disciplina generale, che si adatti nel tempo e che, soprattutto, risulti applicabile in concreto. Sarebbe, infatti, impossibile selezionare e positivizzare specifici strumenti tecnologici da utilizzare nei trattamenti, data l'eterogeneità degli stessi (nonché la possibile influenza al mercato tecnologico che tale scelta comporterebbe); inoltre, legare la normativa a specifiche tecnologie non sarebbe fruttuoso, in ragione dell'obsolescenza tecnologica che li caratterizzerebbe[59].

---

[57] *Ex pluris* cfr. F. CARINGELLA, *La tutela aquiliana della privacy nel Codice per la protezione dei dati personali (d.lgs. n. 196/2003)*, in *Studi di Diritto civile, III, Obbligazioni e responsabilità*, 2007, 719; S. MAZZAMUTO, *Brevi note in tema di mezzi di tutela e di riparto della giurisdizione nelle attività di trattamento dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1998, 249-274; G. RESTA, A. SALERNO, *La responsabilità civile per il trattamento dei dati personali*, in G. ALPA, G. CONTE (a cura di), *La responsabilità d'impresa*, Milano, 2015, 658 *ss*.; M. GAMBINI, *Responsabilità e risarcimento nel trattamento dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I Dati Personali Nel Diritto Europeo*, Torino, 2019, 1017-1081.

[58] Così E.L. GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contratto e impresa*, 2018, n. 1, il quale, commentando il principio di *accountability*, sottolinea che i titolari del trattamento debbano adottare un sistema di controllo della protezione dei dati, strutturato in base a standard di buona amministrazione riconosciuti universalmente e che sia verificabile (*auditable*) all'esterno, in quanto il rispetto delle regole in materia di dati personali da parte dei titolari del trattamento dei dati richiede non il mero adempimento delle disposizioni di legge ma la predisposizione di una vera e propria governance interna: cfr. A. SPINA, *Alla ricerca di un modello di regolazione per l'economia dei dati. Commento al regolamento (Ue) 2016/679*, in *Riv. regolaz. merc.*, 2016, 143 *ss*.

[59] Cfr. S. CALZOLAIO, *Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679,* in *federalismi.it*, 2017, n. 24, 14-17, in Rete: *https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=35361*.

Sempre sul versante delle misure organizzative e tecniche, il Regolamento fa particolarmente affidamento al principio di proporzionalità. Questo, infatti, rappresenta quasi un dogma della disciplina, col quale si intende legare la discrezionalità del titolare, nella scelta delle misure da adottare, a specifici criteri di natura organizzativa ed economica, oltre che a determinate caratteristiche del trattamento [60]. D'altronde, sarebbe del tutto inefficace assegnare rigidi adempimenti astratti, ove non tutti i trattamenti presentino profili di rischiosità tali da necessitare di una particolare strategia (o politica) di prevenzione.

In ragione di ciò, il Regolamento, non prevede un elenco esaustivo né tassativo di misure tecniche ed organizzative adeguate, ma si limita ad indicarne (o prescriverne, a seconda dei casi) alcune, proprio in ragione della discrezionalità che è lasciata al singolo titolare del trattamento. Egli, pertanto, potrà ben mettere in atto non solo le soluzioni 'tipiche' previste dal Capo IV, ma anche configurarne di nuove, purché sempre nel rispetto dei requisiti fissati dal Regolamento[61].

Qui di seguito, pertanto, si andranno ad analizzare i principali strumenti e principi organizzativi che il Legislatore europeo ha previsto che il titolare adotti per assicurare l'applicazione del GDPR.

4.1 Privacy by design e privacy by default

L'articolo 25 introduce il principio di *privacy by design* e *privacy by default*, ossia un approccio concettuale innovativo che impone alle organizzazioni l'obbligo di avviare un trattamento prevedendo, fin da subito, gli strumenti e le corrette impostazioni a tutela dei dati personali.

Il principio della *privacy by design* implica che la protezione dei dati sia integrata nell'intero ciclo di vita di un dato prodotto, servizio o processo, sin dalla relativa progettazione[62]. Diverso, ma complementare principio, è quello della *privacy by default*, il quale implica che il titolare si doti di misure tecniche ed organizzative atte a trattare, per impostazione predefinita (*i.e.* di *default*), solo quei dati personali necessari per ogni specifica finalità del trattamento[63].

La funzionalità di questo approccio regolatorio è data dal fatto che si permette di tutelare la riservatezza dei dati personali in modo duttile, riuscendo a conciliare la

[60] Caratteristiche indicate nello stesso art. 24 GDPR, quali la natura, l'àmbito di applicazione, il contesto e le finalità del trattamento, nonché il rischio di lesione dei diritti e delle libertà delle persone fisiche.

[61] Cfr. G. AMORE, *Fairness, Transparency e Accountability nella protezione dei dati personali,* in *Studium Iuris,* 2020, n.4, 424-426.

[62] Cfr. art. 25 par. 1 GDPR: "*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*".

[63] Cfr. art. 25 par. 2 GDPR: "*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*".

promozione dell'innovazione tecnologica e dello sviluppo di nuovi beni e servizi digitali, con la tutela dei dati e delle informazioni personali. Questi ultimi, difatti sono sempre più spesso necessari per favorire l'innovazione, rendendosi indispensabile raccogliere ingenti quantità di dati per produrre beni o servizi avanzati[64]. In altri termini, nel momento in cui il titolare intenda compiere un qualsiasi trattamento, deve aver già predisposto un sistema tecnico ed organizzativo il quale, prima ancora dall'inizio delle attività, consideri le conseguenze e la portata del trattamento per l'interessato.

Per capire le implicazioni di questo principio è dapprima necessario scrutare, pur sommariamente, quella che è stata l'origine dello stesso. Un primo riscontro della necessità di adottare un approccio volto alla tutela dei dati personali attraverso il *design* dei sistemi informatici lo si trova nei principi generali espressi dal *Department of Health, Education, and Welfare Advisory Committee* nelle *Fair Information Practices Principles* (FIPPs)[65]. Nelle loro varie formulazioni, la tutela della riservatezza, infatti, è stata progressivamente calata nella costruzione e nella gestione dei sistemi informatici che processino dati personali. Si cominciò a comprendere che per garantire una tutela adeguata fosse necessario che lo sviluppo di un sistema informatico dovesse tener in conto, sin dalla progettazione, degli impatti e possibili rischi alla riservatezza dei dati dei soggetti (implementando, altresì, possibili rimedi). Da qui, il concetto di *privacy by design* è stato elaborato a partire dagli anni duemila nell'ambiente dottrinale canadese e, in particolare, grazie alle riflessioni di Ann Cavoukian. L'autrice, infatti, sostenne che per massimizzare l'approccio alla tutela dei dati personali, fosse necessario adottare misure proattive più che reattive (e quindi di risposta), aventi lo scopo di anticipare e prevenire le invasioni della privacy prima che accadano[66]. Operando, pertanto, con un approccio "*before the fact, not after*", si intendeva mirare alla prevenzione da eventuali violazioni della privacy (e in conseguenti sanzioni). Per precisare la metodologia idealizzata, Ann Cavoukian ha elaborato sette principi fondamentali che reggono il suo sistema della privacy[67][68]:

---

[64] Cfr. WP29, *The future of privacy: joint contribution to the Con-sultation of the European Commission on the legal framework for the fundamental right to pro-tection of personal data*, 2009, 12.

[65] Cfr. FEDERAL PRIVACY COMMISION, *Fair Information Practice Principles (FIPPs),* in Rete: *https://www.fpc.gov/resources/fipps/*. In particolare, i principi che le agenzie federali statunitensi dovrebbero rispettare sono: 1. Accesso ed esattezza dei dati; 2. *Accountability*; 3. *Authority*, 4. Minimizzazione, 5. Qualità e integrità, 6. Partecipazione individuale del cittadino, 7. Finalità specifica e uso limitato, 8. Sicurezza, 9. Trasparenza.

[66] Cfr. A. CAVOUKIAN, *Privacy by design, The 7 Foundational Principles*, Canada, 2011.

[67] Cfr. *ivi*, 2.

[68] Cfr. G. BINCOLETTO, *La privacy by design: un'analisi comparata nell'era digitale*, Roma, 2019, 79-81, ove l'autrice fornisce una traduzione dei principi precisa ed esplicativa rispetto al testo originale di Ann Cavoukian, *Privacy by design*. Per completezza, si riporta l'elenco dei principi in lingua originale: "*1. Proactive not reactive: preventative not remedial: The Privacy by Design (Pbd) framework is characterized by the taking of proactive rather than reactive measures. It anticipates the risks and prevents privacy invasive events before they occur. Pbd does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to identify the risks and prevent the harms from arising. In short, Privacy by Design comes before-the-fact, not after. 2. Privacy as the default setting: We can all be certain of one thing — the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice, as the default. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual in order to protect their privacy — it is already*

1. Proattivo non reattivo, preventivo non correttivo: Questo criterio impone l'utilizzazione di metodologie proattive già durante la progettazione di un prodotto tecnologico, per prevenire una violazione e non per dover rimediare ad essa;
2. Privacy come impostazione predefinita: la privacy dev'essere riconosciuta di *default,* senza che sia richiesta un'azione positiva da parte dell'individuo. È necessario assicurare che i dati personali siano automaticamente protetti in ogni sistema ICT e in qualsiasi pratica commerciale;
3. Privacy incorporata nella progettazione: la privacy deve essere integrata nel *design* e così, rappresentare un essenziale componente della funzionalità della tecnologia, essendo appunto inserita nella sua architettura;
4. Massima funzionalità: questo principio intende soddisfare tutti gli interessi e gli obiettivi in gioco, dimostrando che non sempre è imposto scegliere a vantaggio di una singola posizione ed escluderne un'altra, come nel caso della relazione tra privacy e sicurezza;
5. Sicurezza fino alla fine, durante tutto il ciclo del prodotto o servizio: l'approccio deve essere mantenuto per tutta la durata del trattamento dei dati, affinché il dato sia acquisito, trattenuto e distrutto in sicurezza e così la gestione dei dati sia conforme dall'inizio alla fine;
6. Visibilità e trasparenza: la protezione deve essere verificabile dall'individuo grazie alla chiarezza delle misure, nel senso che l'individuo può costantemente controllare che le operazioni sui suoi dati siano conformi alle previsioni e agli obiettivi;
7. Rispetto per la privacy dell'utente, centralità dell'utente: la privacy *by design* richiede che gli individui siano al centro; perciò, devono essere implementate

built into the system, by default. 3. Privacy embedded into design: Privacy measures are embedded into the design and architecture of IT systems and business practices. These are not bolted on as add-ons, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is thus integral to the system, without diminishing functionality. 4. Full functionality: positive-sum, not zero-sum: Privacy by Design seeks to accommodate all legitimate interests and objectives in a positivesum "win-win" manner, not through the dated, zero-sum (either/or) approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is indeed possible to have both. 5. End-to-end security: full lifecycle protection: Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely collected, used, retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end. 6. Visibility and transparency keep it open: Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. The data subject is made fully aware of the personal data being collected, and for what purpose(s). All the component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify! 7. Respect for user privacy: keep it user-centric: Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. The goal is to ensure user-centred privacy in an increasingly connected world. Keep it user-centric".

misure di protezione per impostazione predefinita, la presenza di notifiche appropriate e delle opzioni di policy facili da utilizzare.

Il rilievo dei sopracitati principi ha portato l'approccio della *privacy by design* ad essere diffuso in tutto il mondo, al punto da essere inserito nella proposta di regolamento sulla protezione dei dati personali il cui testo definitivo diventerà il GDPR[69].

Come precedentemente esposto, il concetto di privacy *by design* non rappresenta solo un mero principio astratto, ma un'effettiva prescrizione, che impone la necessaria adozione di un preciso approccio metodologico[70]. Il titolare, infatti, deve compiere delle scelte che, in fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni[71], assicurino la conformità agli adempimenti connessi alla *data protection*. Questa attività comporta un preciso intervento preliminare allo svolgimento del trattamento, in una fase *ex ante* (appunto progettazione e sviluppo), invece che *ex post* (come può essere un servizio di *customer care*). Ciò conduce alla distinzione fra momento *back-end* e *front-end* nella protezione dei dati personali. Infatti, nel momento *back-end*, il *design* riguarda i modi di conservazione e gestione, soprattutto in termini di sicurezza, dei dati in procinto di essere trattati, e deve assicurare il rispetto di quanto previsto a livello legislativo (ed eventualmente contrattuale, nel caso del responsabile del trattamento). Il momento *front-end* invece guarda a quanto avviene nel momento in cui il trattamento è in esecuzione e l'utente, o meglio l'interessato, si interfaccia con il servizio fornitogli o comunque con il trattamento svolto sui suoi dati. In quest'ultimo caso, lo scopo deve essere quello di fornire all'interessato le necessarie informazioni sui dati che verranno acquisiti e di accrescere il controllo dello stesso su esse, garantendo, quindi, un pieno esercizio dei diritti previsti dal Regolamento[72]. In entrambi i momenti, la prospettiva fondamentale della *privacy by design* è quella della sua applicazione

[69] Cfr. considerando n. 61, Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals: "*The protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organizational measures are taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default*", nonché l'art. 23 Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals, contenente l'originario contenuto dell'art. 25 GDPR.

[70] Cfr. S. FAILLACE, *La natura e la disciplina delle obbligazioni id cui all'art. 25 GDPR,* in *Contratto e Impresa*, 2022, n. 4, 1233, ove l'autore, facendo riferimento al report *Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics* (2015)*,* pubblicato dall'ENISA, sottolinea come il concetto di *privacy by design* risulti poliedrico: "*nei documenti giuridici è generalmente descritta in termini molto ampi come principio generale; dagli informatici e dagli ingegneri, è spesso equiparata all'uso di specifiche tecnologie di miglioramento della privacy*", dando atto della prescrittività di tali concetti. A fronte di ciò è necessario evidenziare come l'implementazione della disciplina *data protection,* all'interno dei contesti imprenditoriali, necessiti sempre di un approccio multidisciplinare che permetta di comprendere la fattibilità delle misure giuridiche legislativamente imposte. Il coinvolgimento dei reparti tecnologici ed organizzativi, d'altronde, risulta necessario per tradurre, in termini pratici e operativi, i principi della *privacy by design e privacy by default.*

[71] Cfr. considerando n. 78.

[72] Cfr. A. PRINCIPATO, *Verso nuovi approcci alla tutela della privacy: privacy by design e privacy default setting*, in *Contratto e impresa*, 2015, n. 1, 199-202.

nell'area delle *business practices*, ossia nell'osservare la tutela dei dati personali a livello di *policies* e di prassi aziendali[73]. La valorizzazione di un approccio duale ingegneristico-gestionale, nella gestione della protezione dei dati personali, permette altresì di superare le pratiche di sola implementazione delle *Privacy Enhancing Technologies*[74], che, pur continuando a costituire un valido strumento, non risultano più sufficienti a garantire una corretta attuazione del principio della *privacy by design*.

Un ulteriore aspetto che l'art. 25, par. 1, intende valorizzare è che la scelta delle misure tecniche ed organizzative dev'essere tale da garantire un'efficace attuazione del Regolamento[75], al fine di assicurare i diritti degli interessati. L'efficacia è al cuore del concetto di protezione dei dati fin dalla progettazione[76], determinando l'adozione di misure e garanzie che, auspicabilmente, conseguano l'effetto di protezione dei dati personali. Proprio per l'implementazione delle misure più efficaci, il Legislatore ha dettato una serie di circostanze di cui il titolare deve tener conto nella scelta di quali adottare. In particolare, le misure tecniche ed organizzative da implementare sin dalla progettazione del trattamento devono essere scelte sulla base 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*"[77]. Come intuibile,

[73] Cfr. A. CAVOUKIAN, S. TAYLOR, M.E. ABRAMS, *Privacy by Design: essential for organizational accountability and strong business practices, IDIS 3*, 405–413, 2010.

[74] Con *Privacy Enhancing Technologies* (*PETs*) si intendono tutte le tecnologie orientate all'incremento del controllo sui dati personali inviati e utilizzati da fornitori di servizi online o dell'e-commerce. Le *PETs* mirano alla minimizzazione dei dati personali raccolti e utilizzati, utilizzando, in fase di trattamento, pseudonimi, credenziali di accesso ed ogni altro strumento volto a garantire anonimato e sicurezza dei dati. L'utilizzo delle *PETs* risale alle prime regolazioni in tema di dati personali nel contesto delle ICT come strumento finalizzato alla risoluzione dei problemi inerenti alla privacy. Sull'utilizzo delle PETs, v. J. BORKING; C. RAAB*, Laws, PETs and other technologies for privacy protection,* in *The Journal of Information, Law and Technology*, 2001, 1.

[75] Cfr. art. 25 GDPR: "*misure tecniche e organizzative adeguate […] volte ad attuare in modo efficace i principi di protezione dei dati […] e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati*".

[76] Cfr. EDPB, *Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita*, 2020, 7.

[77] Cfr. *ibidem,* ove l'EDPB fornisce un'interpretazione esaustiva sul contenuto dei citati criteri: 1. il riferimento dello stato dell'arte impone ai titolari di tener conto, nella scelta delle misure tecniche da implementare già dalla progettazione, dei correnti progressi compiuti dalla tecnologia. Lo stato dell'arte è quindi un concetto dinamico, che impone un necessario e costante aggiornamento, da parte del titolare, delle misure adottate ove queste si rilevino obsolete rispetto a nuovi rischi per il trattamento, in termini di protezione dei dati. Trascurare l'aggiornamento sui progressi tecnologici potrebbe, dunque, comportare una mancata osservanza dell'art. 25; 2. il riferimento ai costi di attuazione permette di scegliere le misure tecniche ed organizzative adeguate che risultino le più compatibili con le risorse economiche ed organizzative del titolare. Tuttavia, la valutazione del costo di attuazione delle misure non può mai rappresentare un motivo per astenersi dal realizzare, sin dalla progettazione, la protezione dei dati personali; 3. natura del trattamento, può essere inteso come le caratteristiche intrinseche dello stesso (se sia, ad esempio, caratterizzato tra trattamento di categorie particolari di dati, presenza di processi decisionali automatizzati, …), L'ambito di applicazione fa riferimento alla dimensione e all'ampiezza del trattamento (trattamento su larga scala, *data retention, …)*. Il contesto riguarda le circostanze nel trattamento che possono influenzare le aspettative degli interessati (es. videosorveglianza nei luoghi di lavoro), mentre la finalità si riferisce agli obiettivi del trattamento; 4) infine, la scelta delle misure deve avvenire in relazione a possibili rischi per diritti e libertà degli interessati, nel rispetto, quindi,

oltre a garantire una scelta effettiva delle misure, questi criteri permettono altresì di parametrare le misure adottabili in relazione alla rischiosità del trattamento per i diritti dell'interessato (richiamando il *risk based approach*), nonché alle capacità economiche-aziendali del titolare, il quale è pur sempre tenuto a adottare i mezzi più efficaci. Infine, nel sostenere un quadro proporzionale nell'adozione delle misure tecniche ed organizzative, è da ritenere che questi criteri non debbano essere presi singolarmente per arrivare ad un contesto adeguato, ma che, piuttosto, questi costituiscano dei fattori da considerare all'unisono in vista del raggiungimento dell'obiettivo di creare un contesto *privacy by design.*

Premesso, quindi, che l'adozione di misure tecniche ed organizzative adeguate è fondamentale sin dal momento della determinazione dei mezzi del trattamento, è determinante capire quali possano essere, in concreto, le suddette misure. L'art. 25 del Regolamento evidenzia che tecniche quali la pseudonimizzazione[78] o la minimizzazione dei dati possano essere delle misure tecniche ed organizzative utili per attuare in modo efficace i principi di protezione dei dati. Tuttavia, queste rappresentano solo delle indicazioni esemplificative che possono guidare il titolare nella scelta delle misure da adottare a livello operativo. Ovviamente, questa decisione non può che essere correlata alle circostanze concrete del trattamento di volta in volta considerate, che precludono la possibilità di effettuare un elenco esaustivo delle misure che il titolare potrebbe adottare. Tuttavia, volendo evidenziarne alcune ricorrenti nella prassi[79], il titolare, per soddisfare il principio della *privacy by design,* potrebbe:

- individuare, con anticipo e nello specifico, i dati personali che saranno oggetto di trattamento per mezzo del prodotto, servizio o tecnologia realizzati;
- limitare la raccolta dei dati esclusivamente a quelli realmente necessari per la realizzazione delle finalità perseguite, in ottemperanza al principio di minimizzazione dei dati[80];

---

del sistema *risk-based approach* predisposto dal regolamento. Nell'analizzare i rischi ai fini del rispetto di quanto prevede l'articolo 25, il titolare deve individuare i rischi per i diritti degli interessati associati a una violazione dei principi, e determinare la loro probabilità e gravità al fine di attuare misure efficaci di mitigazione di tali rischi.

[78] L'art. 2, par. 1, n. 5, GDPR, definisce la pseudonimizzazione come "*il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile*".

[79] Cfr. E. FACCIOLI, M. CASSARO, *Il "GDPR" e la normativa di armonizzazione nazionale alla luce dei principi: accountability e privacy by design*, in *Il Diritto industriale*, 2018, n. 6, 563.

[80] Cfr. GPDP, *Registro dei provvedimenti n. 396 del 28 giugno 2018*, in cui il Garante ha constatato l'illiceità del trattamento, per violazione dell'art. 25 GDPR, svolto dal titolare mediante la geolocalizzazione di propri veicoli aziendali, ove non abbia provveduto a progettare il sistema operativo di localizzazione mediante misure adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per la specifica finalità del trattamento. In particolare, il sistema consentiva il monitoraggio continuo dell'attività dei dipendenti senza che gli stessi ne fossero a conoscenza, i dati erano conservati per un periodo di tempo eccessivo rispetto alle finalità del trattamento e, inoltre, i dati di geolocalizzazione venivano raccolti anche ove il dipendente, o un suo familiare, utilizzasse il veicolo al di fuori degli orari di lavoro, in completa violazione, pertanto, del principio di necessità, proporzionalità e minimizzazione dei dati trattati.

- determinare, sin dall'origine, il periodo di conservazione dei dati; tale periodo viene determinato sulla base della durata del trattamento previsto nonché tenendo conto di eventuali obblighi imposti da norme prevalenti[81];
- individuare i dipendenti e/o collaboratori terzi che avranno accesso ai dati personali, al fine di provvedere alla formalizzazione di appositi documenti di nomina, a seconda del caso, a responsabile interno o esterno del trattamento o ad incaricati del trattamento;
- implementare specifiche protezioni che possano mitigare eventi di violazione in seguito ad attacchi informatici esterni o comportamenti illeciti interni, come l'estensiva adozione di tecniche di cifratura delle informazioni 'a riposo' e in transito, di pseudonimizzazione, o di aggregazione dei dati nelle fasi immediatamente successive alla raccolta e direttamente sul sistema di origine[82];
- individuare, ai sensi del GDPR, quei trattamenti che, presentando rischi elevanti per i diritti degli interessati, in quanto trattano una categoria di dato sensibile o presentano un rischio residuo di trattamento elevato, sono soggetti ad una specifica valutazione d'impatto (c.d. DPIA) insieme al parere del DPO;
- infine, in via generale, coinvolgere tutti i dipartimenti soggetti o interessati ai nuovi prodotti e/o servizi nuovi al fine di valutare globalmente l'impatto del trattamento del dato sui singoli processi[83].

A fianco dell'approccio *privacy by design*, il Regolamento accosta il concetto di *privacy by default.* Come illustrato nell'*incipit* del capitolo, l'art. 25, par. 2 GDPR, dispone che il titolare adotti misure adeguate affinché siano trattati di *default* solo i dati necessari per le finalità del trattamento. La protezione per impostazione predefinita, a differenza dell'approccio *by design*, il quale si concentra sulla progettazione del trattamento, focalizza la propria attenzione sullo svolgimento del trattamento, dalla fase della acquisizione dei dati, al periodo di conservazione, sino alla loro possibile condivisione, riutilizzo o cancellazione.

Questo criterio è come se si ponesse in rapporto consequenziale con la *privacy by design*[84], prevedendo che le misure ideate in fase di progettazione del trattamento, siano poi impostate di *default* su ogni dispositivo o sistema, per limitare il trattamento nei termini di quantità di dati raccolti, portata del trattamento, periodo di conservazione dei dati e accessibilità agli stessi. Ciò significa che, per impostazione predefinita, il titolare deve:

---

[81] Cfr. GPDP, *Registro dei provvedimenti n. 348 del 20 ottobre 2022*, in cui il Garante, fra le altre problematiche evidenziate, ha sanzionato Douglas Italia (e ingiunto alla stessa di cancellare i dati risalenti a più di 10 anni addietro) per violazione del principio limitazione della conservazione dei dati, in quanto il titolare del trattamento non ha provveduto a cancellare i dati lasciati per lungo tempo inerti, né a richiedere alcun consenso al trattamento degli stessi (conservazione) per le proprie attività.

[82] Cfr. GPDP, *Registro dei provvedimenti n. 328 del 6 ottobre 2022*, con il quale il Garante ha sanzionato un'impresa, per violazione dell'art. 25 GDPR, per non aver protetto adeguatamente i dati dei clienti registrati nell'area riservata del proprio sito web, poiché utilizzava un protocollo non sicuro ("http") invece che un protocollo crittografato ("https").

[83] Un esempio pratico di come attuare ciò è il *Regolamento Misure tecniche e organizzative relative alla protezione dei dati personali*, 2022, pubblicato dall'Ispettorato Nazionale del Lavoro.

[84] Cfr. F. BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 802-804.

- ridurre al minimo il trattamento dei dati raccogliendo solo quelli strettamente necessari al perseguimento delle finalità;
- non deve conservare i dati trattati per un periodo superiore a quello necessario per le sue finalità o legislativamente previsto;
- offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali;
- consentire all'interessato di controllare il flusso di trattamento dei propri dati[85].

Le misure di protezione e minimizzazione dei dati personali devono essere adottate in automatico dal titolare, senza che l'interessato si attivi per liminare la raccolta dei propri dati.

Un'impostazione di tal genere, si fonda sull'idea che, nel momento di fare una scelta, ove vi sia un'impostazione già preselezionata, le persone tendano a rimanere su quest'ultima, pur avendo la possibilità di cambiare in altre opzioni [86]. Questo comportamento evidenzia, quindi, come le impostazioni di *default* siano fondamentali per la tutela dei diritti degli interessati impattando con estrema forza sulla protezione dei loro dati personali[87]. Avendo garantito uno livello di protezione dei dati predefinito, saranno eventualmente gli stessi interessati a scegliere consapevolmente se condividerne maggiori quantità (o per maggiore tempo) rispetto a quanto prestabilito di *default*[88].

Un ulteriore considerazione sulla *privacy by default* può essere svolta, inoltre, in relazione alla possibile portata applicativa del principio stesso. Alla luce del considerando 78, infatti, la *privacy by default* va ben oltre i titolari dei trattamenti, intesi in senso stretto, estendendosi anche alle attività di progettazione e programmazione dei sistemi e strumenti informatici mediante i quali viene svolto il trattamento[89]. La

[85] Cfr. E. FACCIOLI, M. CASSARO, *Il "GDPR" e la normativa di armonizzazione nazionale alla luce dei principi: accountability e privacy by design,* in *Il Diritto industriale,* 2018, n. 6, 563. Sul punto, inoltre, l'EDPB, nelle *Linee guida 4/2019 sull'articolo 25,* ha specificato alcune misure che possono essere adottate per realizzare per impostazione predefinita (e dalla progettazione) il principio di minimizzazione.

[86] Tale circostanza è stata oggetto di studio della teoria economica del diritto del Paternalismo Libertario. Questa teoria esprime l'idea che sia possibile e legittimo che le istituzioni pubbliche e private influenzino il comportamento delle persone rispettando al tempo stesso la loro libertà di scelta, in quanto tale influenza determinerebbe comunque un beneficio all'individuo o alla collettività. Per approfondire v. P. SILVESTRI, *Economia. Il codice giuridico del mondo*, in A. ANDRONICO, T. GRECO, F. MACIOCE (a cura di), *Dimensioni del Diritto*, Torino, 2019, 418-425.

[87] Un esempio tipico è dato dagli utenti dei *social network.* Si è, infatti, dimostrato come la maggior parte degli utenti tenda a mantenere le impostazioni privacy prestabilite (in particolare, in relazione alla condivisione verso terzi). Da ciò deriva che, se il profilo degli utenti da privato viene reimpostato come pubblico di *default*, la maggior parte di essi condividerà le proprie informazioni personali con una platea ben più ampia di quanto preventivato: v. J. AUSLOOS, E. KINDT, E. LIEVENS, P. VALCKE, J. DUMORTIER, *Guidelines for Privacy-Friendly Default Settings*, in *ICRI Working Paper Series*, n. 12/2013, 15.

[88] Cfr. A. PRINCIPATO, *Verso nuovi approcci alla tutela della privacy: privacy by design e privacy default setting*, in *Contratto e impresa*, 2015, n. 1, 202-204, ove l'autore ritiene che se gli interessati decidessero di modificare le impostazioni di protezione dei dati personali previste di *default* (*in peius* evidentemente), questa scelta avverrebbe in modo (più o meno) consapevole, in quanto i titolari del trattamento, per smuovere i propositi degli interessati, sarebbero costretti a convincere quest'ultimi fornendogli delle informazioni o dei benefici che li spingano a mutare la situazione di *default*.

[89] Cfr. F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, 116. L'autore, infatti, sottolinea come la *privacy by default*, poiché concernente anche "*la progettazione stessa dei trattamenti e degli apparati utilizzati, prima che essi abbiano concretamente avvio, retroagisce*

ragione di questo profondo cambiamento è da rinvenire, più che nella diretta applicazione del Regolamento, nell'influenza indiretta degli obblighi che sono gravanti su titolari e responsabili. Questi ultimi, infatti, dovendo dotarsi di apparati tecnologici che per impostazione predefinita siano conformi alla normativa sulla protezione dei dati personali, compiranno inevitabilmente delle scelte che provocherebbero degli effetti indiretti anche sul mercato e, di conseguenza, sulla creazione degli strumenti informatici e tecnologici, incrementando uno sviluppo della cultura *privacy compliance* sin dalle basi dell'economia digitale[90].

A conclusione, la norma sottolinea, al terzo paragrafo, come i meccanismi di certificazione di cui all'art. 42 GDPR possano essere utilizzati come elemento per dimostrare la propria conformità in tema di *privacy by design* e *by default.* L'utilità delle certificazioni, anche in questo caso, è parallela a quanto evidenziato in relazione all'art. 24, par. 3 del Regolamento: un'attenuazione probatoria del titolare nel dimostrare, in sede di verifica delle autorità di controllo (o in sede giurisdizionale), la propria conformità al GDPR, e in particolare all'art. 25[91].

Prescindendo dagli effetti dati dal Regolamento, la predisposizione di meccanismi di certificazione della *privacy by design* permetterebbe di mitigare l'incertezza nella scelta delle misure da realizzare, contribuendo ad evidenziare l'attuale "stato dell'arte" nello specifico ambito di applicazione del trattamento. Pur essendo le interpretazioni delle autorità di controllo, dell'EDPB o delle stesse corti rilevanti nel concretizzare questo principio, è da riconoscere come siano gli operatori attivi nella prassi i soggetti più qualificati a definire, nel dettaglio, le misure più appropriate da poter applicare per dare attuazione a questi principi. Su tali premesse, sarebbe, quindi, corretto reputare che, ove sussistano certificazioni (o in generale codici di condotta, *best practices,* …) che prevedano un livello elevato di protezione per l'interessato in conformità (o in misura superiore) ai requisiti giuridici, i titolari dovrebbero tenerne conto nella progettazione e nell'attuazione delle misure di protezione dei dati.

In questo modo lo strumento certificativo comporterebbe un salto di qualità per le imprese, risultando il più appropriato ad assicurare che la *privacy by design* possa essere, oltre che un elemento di sicurezza, una condizione di incentivo per i soggetti commerciali. I benefici che ne potrebbero derivare, infatti, rileverebbero in termini sia di maggior tutela degli interessati, sia di minor rischio (e minori esborsi) del titolare, che certifichi un proprio trattamento, di essere esposto ad azioni legali o procedimenti sanzionatori che comportino ingenti sanzioni pecuniarie o condanne al risarcimento del danno.

---

naturalmente anche sulla progettazione degli strumenti e delle applicazioni finalizzate a trattare dati personali".

[90] Con il Regolamento, infatti, si ha un evidente mutamento di approccio della politica regolatoria europea sulle nuove tecnologie, in cui non è più il legislatore a seguire l'evoluzione tecnologica, ma sono queste ultime a dover essere, sin dall'origine della fase di progettazione, conformi al dettato normativa.

[91] Cfr. EDPB, *Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita, 2020*, *30 ss*., ove si evidenzia che "*laddove un trattamento svolto da un titolare o un responsabile sia stato certificato ai sensi dell'articolo 42, le autorità di controllo ne tengono conto nella loro valutazione della conformità con il RGPD, in particolare con la DPbDD. […] Anche qualora un trattamento sia certificato ai sensi dell'articolo 42, il titolare è comunque tenuto a garantire il monitoraggio costante e il miglioramento della conformità ai criteri della DPbDD di cui all'articolo 25*".

Come si illustrerà in seguito, la certificazione non copre l'intero ciclo del trattamento dei dati, ma solo un segmento di esso. Tale circostanza determina necessariamente che si specifichi, già da questo capitolo, quali elementi del trattamento costituirebbero oggetto di certificazione *privacy by design* e *by default*. In particolare, gli elementi che contribuiscono ad attestare la conformità del trattamento all'articolo 25, par. 1 e 2 "*sono le procedure di progettazione, ossia la procedura per determinare i mezzi di trattamento, la governance, nonché le misure tecniche e organizzative finalizzate ad attuare i principi di protezione dei dati*"[92].

4.2 Il Registro delle attività di trattamento

Fra gli adempimenti principali del titolare del trattamento, l'art. 30 prevede la tenuta del registro delle attività di trattamento[93]. Si tratta di un documento contenente le principali informazioni relative alle operazioni di trattamento svolte dal titolare. Tale strumento, contribuisce, pertanto, a rafforzare l'*accountability* del titolare, in quanto idoneo a fornire un quadro globale e aggiornato dei trattamenti posti in essere all'interno della propria organizzazione, al fine, anche, di carpire dal contesto organizzativo eventuali criticità o profili di miglioramento su cui sia opportuno intervenire. In tal modo, il registro è uno strumento fondamentale per le attività di valutazione e analisi dei rischi che possono presentare i vari trattamenti, permettendo di verificarne la conformità al Regolamento, nonché per diffondere consapevolezza e condivisione interna all'organizzazione del titolare, potendo essere posto alla base di eventuali *policy* interne.

Il GDPR prevede due distinte tipologie di registri delle attività di trattamento: uno in capo al titolare e uno al responsabile del trattamento, il quale, ove nominato, è tenuto

[92] Cfr. *ibidem.*

[93] Cfr. art. 30 Registri delle attività di trattamento: "*1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni: a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati; b) le finalità del trattamento; c) una descrizione delle categorie di interessati e delle categorie di dati personali; d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali; e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate; f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati; g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1. 2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente: a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati; b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento; c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate; d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1. […]*".

a formare un registro di tutte le attività relative al trattamento svolte per conto di un determinato titolare. Inoltre, in caso di pluritititolata di un trattamento, si ritiene che lo stesso debba essere censito nei registri di tutti i co-titolari o co-responsabili del trattamento.

In relazione ai contenuti, il registro deve includere l'annotazione di svariate informazioni inerenti ai trattamenti svolti in una data organizzazione, fra cui i dati trattati, le finalità, eventuali soggetti destinatari, eventuali trasferimenti verso paesi terzi o organismi internazionali, nonché le garanzie adeguate adottate, le modalità di analisi e 'uso' dei dati e le misure di sicurezza previste per il trattamento; inoltre, nel caso del registro del responsabile, egli deve dare indicazione anche del titolare per cui i trattamenti sono svolti.[94]

Questione controversa, in dottrina, è l'obbligatorietà di questo adempimento. Infatti, il Legislatore europeo si è espresso, nel considerando n. 82, prospettando l'ideale per cui tutti i titolari e responsabili del trattamento si dotassero di un registro al fine di garantire un controllo sulle attività di trattamento compiute e di cooperare con le autorità di controllo. Questo postulato è stato poi trasposto nell'art. 30, dove al paragrafo 5, il Legislatore stabilisce l'obbligatorietà del registro per gli organismi che hanno un numero di dipendenti superiore a 250, nonché per qualunque titolare o responsabile che, pur avendo un numero inferiore di dipendenti, svolga trattamenti che possano presentare un rischio per l'interessato, che effettui trattamenti non occasionali, o che tratti dati relativi alle categorie particolari di cui all'art. 9 GDPR, o di dati giudiziari. Per la dottrina, pur essendo il registro uno strumento necessario per realizzare un contesto del trattamento *accountable*, la portata della deroga di cui al par. 5 vanificherebbe il principio di proporzionalità, su cui l'intero impianto normativo dovrebbe fondarsi, oltre che l'esenzione dimensionale prevista dalla norma a favore delle PMI[95]. In questo modo, infatti, l'esenzione sarebbe del tutto marginale (se non isolata), in quanto, ove semplicemente ricorra una delle tre ipotesi, una PMI sarebbe tenuta a redigere il registro dei trattamenti, con evidenti costi dal punto di vista economico e organizzativo[96]. Nonostante ciò, il WP29 ha precisato che è sufficiente che

[94] Sul punto, il Garante italiano ha dettagliatamente precisato le informazioni che devono essere contenute nel registro del titolare e responsabile del trattamento, in Rete: *https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento*.

[95] Cfr. L. BOLOGNINI, *Obbligo di documentazione*, in C. BISTOLFI, L. BOLOGNINI, E. PELINO (a cura di), *Il Regolamento Privacy Europeo*, Milano, 2016, 413 *ss.;* G. ARCELLA*, GDPR: il Registro delle attività di trattamento e le misure di accountability,* in *Notariato*, 2018, n.4, 393-395; M. CASTELLANETA, *L'incidenza del regolamento GDPR sul quadro normativo esistente,* in *Notariato*, 2018, n. 3, 264.

[96] In particolare, v. M. MASSIMINI, *Il registro dei trattamenti GDPR e la deroga fantasma per le PMI,* in *Privacy.it*, 2018, in Rete: *https://www.privacy.it/2018/04/27/massimini-registro-trattamenti-gdpr-deroga/*, ove l'autore sottolinea apertamente l'insensatezza dell'apparato normativo esistente in tema di registro dei trattamenti, ritenendo che *"Sia l'art. 30 che il Position Paper del WP 29 non sembrano aver tenuto in alcun modo conto della specifica situazione delle micro, piccole e medie imprese. Allo stato attuale delle cose, sia una lettura piatta del par.5, sia l'interpretazione autentica fornita dal WP 29, suggeriscono alle PMI con meno di 250 dipendenti di istituire e mantenere il registro dei trattamenti se vogliono esser certe di non violare un obbligo di legge e rischiare di incorrere (magari per questo solo motivo) nelle temibili sanzioni del GDPR. Anche perché, in questo scenario interpretativo, le ipotesi concrete in cui si possa davvero godere dell'esonero dall'obbligo di tenuta del registro sono davvero remote"*.

occorra una sola delle condizioni previste dall'articolo 30 per far scattare l'obbligo di tenuta del registro, eliminando, ogni dubbio in merito[97].

Quanto agli obblighi di gestione, è indispensabile che il registro abbia forma scritta, anche mediante stesura in formato elettronico. La sua compilazione *una tantum*, tuttavia, non determina l'adempimento dell'obbligo, in quanto questo dev'essere aggiornato, sia nei contenuti, che negli elementi informativi di cui si compone.

Da questo punto di vista, la prima stesura del registro del trattamento, si rileva essenziale per mappare i flussi di dati all'interno dell'organizzazione del titolare, mentre successivamente, diviene un elemento centrale per delineare il quadro generale del sistema privacy del titolare. Per questo motivo, è determinante conservare le precedenti versioni dei registri con le informazioni sui trattamenti relative ad un determinato periodo temporale, al fine di agevolare gli eventuali controlli delle autorità ispettive competenti, nonché per evidenziare gli aggiornamenti nelle misure di sicurezza apportate al trattamento.

Proprio perché il registro dovrebbe determinare una gestione trasparente dei flussi informativi, una sua stesura completa e aggiornata, dovrebbe essere un punto focale per l'ottenimento di una certificazione o l'adesione ad un codice di condotta. La chiarezza organizzativa data dal registro, infatti, garantirebbe un'agevole verificabilità dei trattamenti svolti dal titolare verso *audit* esterni.

4.3 Valutazione d'impatto sulla protezione dei dati personali (*Data protection impact assesment*)

Nel *framework* degli adempimenti necessari per soddisfare il principio di *accountability*, e in esecuzione del principio della *privacy by design,* il Regolamento impone ai titolari del trattamento di compiere una valutazione delle conseguenze delle proprie operazioni sui diritti e le libertà delle persone fisiche mediante una valutazione d'impatto sulla protezione dei dati personali (nella terminologia inglese *Data Protection Impact Assesment*, in acronimo DPIA). Il GDPR non definisce formalmente il concetto di valutazione d'impatto, tuttavia, questa può essere indentificata come un procedimento inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli. Le DPIA sono strumenti importanti per la responsabilizzazione, in quanto sostengono i titolari del trattamento non soltanto nel rispettare i requisiti del GDPR, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento[98].

---

[97] Cfr. WP29, *Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR,* 2018, in Rete: *https://ec.europa.eu/newsroom/article29/items/624045/en*.

[98] Cfr. WP29, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679, 17/IT WP 248 rev.01*, 2017, in Rete: *https://ec.europa.eu/newsroom/article29/items/611236/en.*

La realizzazione di una DPIA è fondamentale in quanto garantisce un approccio metodologico che permette: *ex ante* al trattamento, di ideare misure tecniche ed organizzative adeguate utili a trattare i dati personali in conformità al regolamento, permettendo di individuare, analizzare, stimare, valutare, attenuare e riconsiderare i rischi elevati per i diritti e le libertà degli interessati connessi al trattamento dei loro dati personali; *ex post,* invece, di avere uno strumento di *compliance* e documentazione adeguata utile a dimostrare, in sede di eventuali contestazioni amministrative o giudiziali, che i trattamenti siano stati effettuati rispettando diligentemente i principi del regolamento.

In tale frangente, l'obbligo per i titolari del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati va inteso nel contesto dell'obbligo generale di gestire adeguatamente i rischi presentati dal trattamento di dati personali. Va sottolineato, però, che quella di valutazione dei rischi ai diritti e alle libertà degli interessati del trattamento non è una singola attività, ma in obbligo incessante; i titolari del trattamento, infatti, devono continuamente valutare i rischi creati dalle loro attività al fine di stabilire quando una tipologia di trattamento possa presentare un rischio elevato.

Segnato da tali presupposti, è evidente come l'art. 35 GDPR sia una finestra sul sistema *risk based approach* creato dal Legislatore per promuovere, se non il migliore, il più corretto trattamento dei dati personali. La DPIA, infatti, sottolinea i concetti di "rischio" e "gestione del rischio", prevedendo come presupposto che, quando un trattamento presenti un rischio elevato ai diritti e libertà degli interessati, a causa della natura, l'oggetto, il contesto o le finalità del trattamento, o per l'uso di nuove tecnologie, il titolare del trattamento debba fare una valutazione di impatto sulla protezione dei dati trattati.

Pur essendo la norma apparentemente chiara, in realtà, è fonte di alcune incertezze: come fare, infatti, a capire quando un trattamento possa produrre un rischio elevato? Certo, lo stesso articolo, insieme ai 'considerando', specifica che, "*in particolare presentano un alto rischio: 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; c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico*"[99], tuttavia questo, in realtà, rappresenta solo un elenco esemplificativo e non sicuramente esaustivo. Vi possono essere attività di trattamento a "rischio elevato" che non trovano collocazione in tale elenco ma che presentano tuttavia rischi altrettanto elevati, la cui individuazione è però rimessa al titolare di volta in volta coinvolto.

A fronte di tale problematica sono più volte intervenute le autorità di controllo nazionali e gli organismi europei nell'ottica di chiarire quando un trattamento presenti un rischio elevato. In particolare, l'EDPB, con le "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*", ha

[99] Cfr. art. 35, par. 3 e considerando nn. 71,75,76,92,116.

precisato che, nell'individuazione dei trattamenti che presentino un rischio elevato bisogna considerare nove criteri:

1. valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato"[100];
2. trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che "hanno effetti giuridici" o che "incidono in modo analogo significativamente su dette persone fisiche";
3. monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico";
4. presenza di dati sensibili o dati aventi carattere altamente personale: i primi chiaramente identificabili come quelli definiti dall'art. 9 (particolari categorie di dati) o dall'art. 10 (dati su condanne penali o reati) del regolamento, mentre i secondi possono essere considerati come sensibili perché legati ad attività a carattere personale o domestico oppure perché influenzano l'esercizio di un diritto ovvero perché la loro violazione implica gravi ripercussioni sulla vita quotidiana dell'interessato;
5. trattamento di dati su larga scala: tale è il trattamento per 1) il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; 2) il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; 3) la durata, ovvero la persistenza, dell'attività di trattamento; 4) la portata geografica dell'attività di trattamento;
6. creazione di corrispondenze o combinazione di insiemi di dati;
7. dati relativi a interessati vulnerabili: i minori, i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento;
8. uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative: l'uso di nuove tecnologie, infatti, può comportare nuove forme di raccolta e di utilizzo dei dati, generando nuovi possibili rischi per i diritti e le libertà delle persone, anche sconosciuti, che potrebbero avanzare conseguenze significative;
9. quando il trattamento in sé "*impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto*"[101]: Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto.

A fronte di tali parametri, quindi, ove soddisfatti uno o più, il titolare del trattamento dovrà eseguire una valutazione d'impatto per essere *compliance* ai propri obblighi. Tuttavia, la valutazione del grado "elevato" di rischio dev'essere svolta oggettivamente e non è sempre detto che, qual ora il trattamento ricada in uno dei già

[100] Cfr. considerando n. 71 e 91.
[101] Cfr. art. 22 e considerando n. 91 GDPR.

menzionati casi debba essere sempre considerato ad alto rischio; il titolare, infatti, potrebbe ben considerarlo tale da non presentare un rischio elevato. A questo punto, però, scatterebbero a suo carico una serie di oneri giustificativi ulteriori che gli permettano di documentare i motivi che lo hanno spinto a non effettuare la DPIA.

Anche i criteri individuati dall'EDPB, però, non risultano esaustivi; ad esempio, non si menziona, come trattamento rischioso, quello per cui sia previsto un trasferimento transfrontaliero di dati al di fuori dei confini dell'UE, potendo questo comportare un notevole aumento del rischio per l'interessato nell'esercitare il proprio diritto alla protezione dei dati. È per tale ragione che si rende essenziale anche la prassi delle autorità di controllo. Infatti, il Legislatore europeo ha previsto che l'autorità nazionale di controllo possa redigere un elenco delle tipologie di trattamenti per cui la DPIA è sempre obbligatoria, alleviando, di conseguenza, i dubbi interpretativi che potevano sorgere ai titolari in merito ai casi in cui la DPIA dovesse essere effettuata.

Altro elemento di supporto è altresì la procedura di consultazione preventiva; in questo modo l'autorità Garante assume anche un ruolo consultivo, oltre che meramente sanzionatorio. Nella procedura di consultazione l'autorità di controllo nazionale potrà, qual ora il titolare si rappresenti che la valutazione d'impatto non è sufficiente a individuare o contenere tutti i rischi per l'interessato, fornire un parere sulla valutazione d'impatto da quest'ultimo svolta nonché sugli eventuali correttivi che possono essere attuati dal titolare per attenuare il rischio del trattamento svolto.

Di notevole importanza, infine, risulta l'attività interpretativa delle autorità garanti, derivante dalle raccomandazioni e dai provvedimenti sanzionatori[102]. Uno fra gli ultimi esempi è il provvedimento n. 409 dd. 1° dicembre 2022 dell'autorità italiana Garante per la protezione dei dati personali, la cui massima è riassumibile nel fatto che comporta rischi specifici per i diritti e le libertà degli interessati, nel contesto lavorativo, il trattamento dei metadati relativi all'utilizzo della posta elettronica, consistente nella sistematica raccolta di tali metadati, nella memorizzazione per 180 giorni e nella possibilità di effettuare estrazioni, elaborazioni e verifiche su tali metadati, tanto più in considerazione della particolare 'vulnerabilità' degli interessati nel contesto lavorativo[103].

---

[102] Sul ruolo dell'Autorità Garante nel sistema multilivello delle fonti, v. C. COLAPIETRO, *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello. Il regolamento UE 2016/679 parametro di legittimità della complessiva normativa sulla privacy*, Napoli, 2018, 107-108. L'autore, infatti, osserva che l'Autorità garante della privacy *"è chiamata a mettere a sistema quegli elementi di flessibilità che il regolamento contiene e che la legislazione italiana esalta"*.

[103] V. GPDP, *Ordinanza di ingiunzione nei confronti di Regione Lazio, reg. prov. n. 409 dd. 1° dicembre 2022,* in Rete: *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9833530*. Nel caso di specie, l'autorità Garante ha sanzionato la Regione Lazio per l'illecito trattamento dei metadati relativi all'utilizzo della posta elettronica dei dipendenti, effettuato in assenza di una preliminare valutazione d'impatto sulla protezione dei dati sul presupposto che il trattamento non presentasse rischi specifici per gli stessi. Il trattamento in questione, consistente nella sistematica raccolta di tali metadati (incluse le informazioni relative al mittente/destinatario e all'oggetto di ciascuna e-mail), nella memorizzazione per 180 giorni e nella possibilità di effettuare estrazioni, elaborazioni e verifiche su tali metadati, comporta rischi specifici per i diritti e le libertà degli interessati nel contesto lavorativo. Tanto in considerazione della particolare vulnerabilità degli interessati nel contesto lavorativo (cfr. cons. 75, art. 88 del GDPR e le Linee guida sulla DPIA, che, tra le categorie di interessati vulnerabili, menzionano espressamente "*i dipendenti*") e del fatto che in tale ambito l'impiego di sistemi che comportano il

Ulteriore interrogativo che emerge dalla lettura dell'art. 35 è quale debba essere, in concreto, il contenuto della valutazione d'impatto e quali siano le metodologie per realizzarla. Il testo normativo, infatti, prevede un contenuto minimo indicato in via generica disponendo come necessaria: "*1. una descrizione dei trattamenti previsti e delle finalità del trattamento; 2. una valutazione della necessità e proporzionalità dei trattamenti; 3. una valutazione dei rischi per i diritti e le libertà degli interessati; 4. le misure previste per: o affrontare i rischi o dimostrare la conformità al presente regolamento*". In realtà, il predetto elenco dei contenuti della DPIA segna anche la definizione della procedura medesima che, a sua volta, riprende il modello tradizionale *risk based* per l'analisi del rischio, ovvero: 1) analisi del trattamento; 2) identificazione e valutazione dei rischi connessi al trattamento analizzato; 3) definizione delle misure correttive o idonee a mitigare i rischi individuati (d'altronde, come evidenziato nel precedente capitolo, il rischio non si può mai completamente eliminare ma solo attenuare in modo più o meno significativo).

Come, poi, sensibilmente sostenuto, la fase relativa all'analisi del rischio comprende poi due diversi tipi di valutazioni: la disamina della "*necessità e proporzionalità*" del trattamento dei dati e l'indagine circa i "*rischi per i diritti e le libertà delle persone*". Queste due valutazioni sono correlate e conseguenti, poiché, in termini generali ed a maggior ragione in presenza di un eventuale rischio, qualora l'elaborazione dei dati risulti non necessaria o sproporzionata, nemmeno si pone un problema di analisi del rischio. In tale ipotesi, infatti, coerentemente con l'esigenza di bilanciamento degli interessi in concreto contrapposti, il trattamento non sarà realizzabile, poiché eccedente rispetto alla finalità perseguita, a meno che lo stesso non venga previamente ridimensionato in rapporto a detta finalità[104].

In questi termini, quindi, la valutazione dell'esistenza di rischi elevati per gli interessati deve avere una lettura qualificata verso il rispetto anche degli altri principi del GDPR, quale limitazione delle finalità e minimizzazione, in quanto la violazione degli stessi è comunque suscettibile di incidere sui diritti fondamentali degli individui. In tal senso, una migliore progettazione della DPIA dovrebbe concentrarsi sull'impiego concreto che sarà effettuato dei dati trattati da parte del titolare, slegandosi da valutazioni preventive ed astratte, in quanto significativamente inattendibili.

L'utilizzo di certificazioni avrebbe un immediato vantaggio, ossia garantire l'adozione di modelli valutativi adeguati utili sia a conseguire la certificazione in oggetto, sia ad effettuare una valutazione d'impatto effettiva, completa e ponderata verso, almeno, quei trattamenti che saranno oggetto di verifica in sede di procedimento certificativo. I criteri per i meccanismi di certificazione, difatti, potrebbero, prendere ad oggetto (anche in ottica di semplificazione) i contenuti di cui all'art. 35, specificandoli ulteriormente in base ai settori produttivi in cui verrebbero trattati i dati, o comunque in relazione ad altre circostanze, eliminando il senso di incertezza che ruota attorno ai

"*monitoraggio sistematico*", inteso come "*trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti*" (cfr. criterio n. 3 indicato nelle Linee guida cit., ma vedi anche criteri 4 e 7), può presentare rischi, come emerso nel caso di specie, in termini di possibile monitoraggio a distanza dell'attività dei dipendenti.

[104] Cfr. A. MANTELERO, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Le Nuove Leggi Civili Commentate*, 2017, n. 1, 144-164.

criteri e contenuti della DPIA e permettendo ai titolari del trattamento di avere uno strumento preciso su cui, poi, sviluppare la valutazione dei rischi del trattamento. In questo modo le conseguenze dirette di una tale metodologia sono evidenti: *ex ante* al trattamento, ottenere la documentazione idonea a dimostrare la propria *compliance*; *ex post*, invece, garantire, verso non solo le istituzioni, ma anche verso gli interessati, il fatto che i loro dati siano trattati lecitamente ed in modo da attenuare ogni possibile (e prevedibile) rischio verso i loro diritti e libertà, determinando tutta una serie di vantaggi commerciali.

4.4 La sicurezza nel trattamento e la gestione dei *data breach*

La sicurezza rappresenta un elemento fondamentale nel trattamento dei dati personali. L'importanza e l'accresciuta sensibilità alla questione della sicurezza dei dati personali, data dallo sviluppo del mercato digitale e dall'evoluzione delle tecnologie, è dovuta anche dall'influenza che le stesse tecnologie hanno sulle persone e nella conseguente fiducia che queste ripongono nell'ambiente online[105]. Ovviamente, questo livello di fiducia nelle tecnologie può essere mantenuto solo assicurando un sistema di garanzie e tutele adeguato alla salvaguardia dell'integrità dei dati personali.

Proprio per consolidare la fiducia dei cittadini europei nel trattamento e circolazione dei dati personali, il Regolamento, già nel delineare i principi fondamentali, assegna autonoma importanza all'integrità e alla riservatezza dei dati, così come delineato dall'art. 5, par. 1, lett. f)[106]. La sicurezza deve coprire ogni fase del trattamento e dev'essere rivolta a garantire la protezione dei dati da trattamenti non autorizzati o illeciti, dalla perdita degli stessi, dalla distruzione o dal danno accidentale.

La sicurezza del trattamento dev'essere garantita già a partire dall'architettura dello stesso. I principi della *privacy by design* e *by default,* infatti, presidiano la predisposizione da parte del titolare di misure organizzative e tecniche rivolte a garantire, oltre che l'efficace attuazione dei principi del Regolamento, anche la predisposizione di un'infrastruttura sicura, resistente e resiliente. Questo comporta tanto al titolare, quanto al responsabile del trattamento, di disporre misure adeguate a garantire un livello di sicurezza commisurato ai rischi cui sono esposti i dati personali trattati. L'assunzione di misure di sicurezza, pertanto, non è demandata ad una semplice disposizione, ma ad un complesso articolato normativo che nel suo insieme garantisce la predisposizione di un sistema di *cybersecurity* e protezione dei dati personali[107].

---

[105] Il tema della sicurezza dei dati personali è, infatti, divenuto fondamentale sia per l'Agenda digitale europea (v. COMMISSIONE EUROPEA, *COM/2010/245, "Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni – Un'agenda digitale europea", 2010*) sia, in generale, per la strategia europea dei dati.

[106] Cfr. considerando n. 39 GDPR: "*I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento*".

[107] Oltre agli artt. 32 e 33-34 del Regolamento, di cui si dirà in seguito, non può che farsi riferimento alle norme principali che regolano gli strumenti di *accountability* del titolare e responsabile del trattamento, ossia all'art. 24 (ove si richiede al titolare di adottare misure tecniche ed organizzative idonee ad assicurare la conformità del trattamento), nel richiamato art. 25 (nel predisporre, sin dalla progettazione,

Nuovamente viene in rilievo la gestione del rischio connesso al trattamento, che diventa, anche in questo caso, il parametro di verifica dell'adeguatezza delle misure di protezione predisposte. In particolare, le misure di sicurezza che titolare e responsabile del trattamento devono implementare sono strettamente correlate ai possibili rischi incidenti alla sicurezza del trattamento. In questo caso, tuttavia, la gestione del rischio non è direttamente rivolta ad evitare che l'interessato possa andare in contro a pregiudizi dati da trattamenti illeciti. Il rischio, nella gestione della sicurezza dei dati, concerne i dati stessi e le infrastrutture informatiche su cui sono conservati (e quindi trattati).[108] Su questo fronte, i rischi che un trattamento può presentare possono concernere la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati.

È evidente che tali *incident* [109] possano anche arrecare un pregiudizio all'interessato ma questo aspetto rappresenta, piuttosto, una conseguenza derivata della violazione delle misure di sicurezza previste a protezione dei dati personali predisposte dal titolare o dal responsabile del trattamento. Anzi, bisogna sottolineare che non è sempre detto che una violazione dei dati personali possa comportare una lesione all'interessato; ciò, infatti, è evincibile nel fatto che il Regolamento non onera il titolare o il responsabile ad informare della violazione l'interessato, ove questa non presenti un rischio per i diritti e le libertà di quest'ultimo.

Come sopraindicato, l'art. 32 del GDPR richiede che venga assicurato un livello di sicurezza adeguato ai rischi derivanti dal trattamento. L'articolo in oggetto, dunque, come per gli altri adempimenti connessi al principio di *accountability,* lascia ampia libertà al titolare o responsabile del trattamento nella scelta delle misure da adottare, limitandola solo in relazione ad una serie di criteri guida: lo stato dell'arte, i costi di attuazione, la natura, l'oggetto, il contesto, le finalità del trattamento[110], nonché i rischi di varia probabilità e gravità per i diritti e le libertà degli interessati[111]. Sul punto, il Legislatore europeo fornisce, in via esemplificativa, una serie di misure tipiche che possono essere adottate per assicurare la sicurezza e l'integrità dei dati:

1. la pseudonimizzazione dei dati personali[112];

---

e per impostazione predefinita, un sistema di sicurezza adeguato a proteggere i dati trattati) e negli artt. 35 e 36 (in materia di DPIA e di consultazione preventiva).

[108] Cfr. F. ROTOLO, *Articolo 32 – Sicurezza del trattamento*, in E. BELISARIO, G.M. RICCIO, G. SCOZZA (a cura di), *GDPR e Normativa Privacy*, Milano, 2020, 373-384.

[109] Il termine "incidente" o "*incident*" descrive "*un evento patologico rispetto alla fisiologica operatività di un servizio o di un processo, idoneo in quanto tale a determinare (sia pure a livello meramente potenziale) una non conformità normativa oppure una riduzione della qualità del medesimo servizio o processo*". Cfr. V. FANCELLO, *Certificazione dei corrispettivi elettronici: processi, tecnologie e punti di controllo IT*, in *Amministrazione & Finanza*, 2019, n. 12, 62-63.

[110] Per il significato di tali concetti v. nota 77.

[111] In questo senso, uno strumento utile per vagliare l'adeguatezza delle misure rispetto ai rischi del caso concreto è la DPIA. All'esito della valutazione, infatti, il titolare potrebbe prendere in considerazione di adottare delle ulteriori misure, opportunamente correlate al rischio riscontrato nello specifico trattamento.

[112] Per il significato della pseudonimizzazione v. nota 78. Inoltre, per un approfondimento sul tema della pseudonimizzazione l'Agenzia dell'Unione europea per la cybersicurezza ha pubblicato un report relativo alle tecniche di pseudonimizzazione in cui fornisce esempi pratici in cui queste tecniche possono essere applicate (v. ENISA, *Tecniche di pseudonimizzazione e migliori pratiche*, 2019).

2. la cifratura dei dati personali: la cifratura dei dati, mediante apposita criptografia, permette di rendere incomprensibile i dati a chiunque non sia autorizzato ad accedervi[113];
3. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento[114];
4. la capacità di rispristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
5. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento[115].

Ovviamente, ove ne siano necessarie ulteriori, il titolare non si può limitare a adottare solamente le misure tecniche ed organizzative indicate dalla norma ma dovrà disporne di ulteriori – anche di natura atipica – allo scopo di assicurare la sicurezza e l'integrità dei dati[116]. Ulteriori misure, poi, potranno essere eventualmente adottate dal titolare in sede di procedure con la finalità di intraprendere un percorso per l'adesione a specifici codici di condotta o schemi di certificazione. Ciò con la finalità di attestare l'adeguatezza delle procedure di sicurezza del trattamento prescelte, precostituendosi delle 'prove' per l'accertamento della propria conformità[117].

Oltre all'adozione di misure di sicurezza tecniche, è importante che il titolare e responsabile del trattamento si dotino di un'adeguata procedura di gestione degli eventi che possano mettere a repentaglio la sicurezza dei dati personali. L'adeguata formazione del personale nel corretto utilizzo dei *devices* coinvolti dai trattamenti e la predisposizione di precise ed adeguate *data breach policy* (o quant'altri simili disciplinari interni) possono essere due misure organizzative che permetterebbero di agire tempestivamente, e con cognizione, per contenere la violazione o, quantomeno, per evitare che si verifichino ulteriori violazioni a conseguenza dell'inefficienza

[113] La differenza fra la cifratura/criptografia e la pseudonimizzazione è che la prima oscura tutte le informazioni sostituendo integralmente i dati con qualcos'altro, relazionato solamente alla chiave criptografica; la pseudonimizzazione, invece, consente a chiunque abbia accesso ai dati di visualizzare parte del set di dati, pur non potendo ricondurre tutti i dati ad un determinato interessato. Ovviamente pseudonimizzazione e crittografia possono essere usate contemporaneamente, garantendo, in questo modo, un livello di cifratura elevato in quanto, oltre a separare i dati personali di un dato soggetto in diversi *set* di dati, permettendo la completa identificazione dell'interessato solo mediante un codice di collegamento, si cifrano altresì tutti i diversi set, modificando i dati in esso contenuti in un contenuto tendenzialmente illeggibile (e quindi non fruibile) da parte di terzi non autorizzati. Per approfondire v. D. STEFANELLO, *Come proteggere i dati personali? Anonimizzazione, pseudonimizzazione e cifratura a confronto,* in *Ius in itinere*, 2022, in Rete: *https://www.iusinitinere.it/come-proteggere-i-dati-personali-anonimizzazione-pseudonimizzazione-e-cifratura-a-confronto-17616*.

[114] Ad esempio, mediante *antivirus, firewall,* sistemi di *backup* e *recovery,* misure di segmentazione dei dati e delle reti, gruppi di continuità, ed altro.

[115] Ad esempio, mediante un *penetration test,* cioè un attacco informatico simulato autorizzato su un sistema informatico o una rete, eseguito per valutare la protezione del sistema.

[116] In proposito, l'ENISA, nel 2021, ha pubblicato due *vademecum* dedicati alle PMI per evidenziare le misure di sicurezza e *policy* necessarie per affrontare la sicurezza informatica che possono fungere da linee guida per quanto concerne l'implementazione delle politiche di sicurezza: *cybersecuirity for SMEs – Challenges and Recommendation* e *cybersecurity guide for SMEs – 12 steps to securing your business*.

[117] Sul punto v. *infra* 100.

organizzativa, causando un pregiudizio ulteriore agli interessati[118]. Un ulteriore misura organizzativa adottabile per assicurare la sicurezza dei dati personali trattati è l'effettiva implementazione del principio di minimizzazione. Infatti, minimizzare la quantità di dati raccolti, l'estensione del trattamento, il periodo di conservazione e l'accesso ai dati stessi determinerebbe minori rischi all'interessato, con riferimento sia all'entità del danno che eventualmente si produrrebbe in caso di violazione dei dati personali, sia alla probabilità del verificarsi di un evento lesivo[119].

Tutte le misure elencate sono finalisticamente rivolte ad evitare l'evento del *data breach*. Con tale termine si identifica ogni violazione di sicurezza che comporti, 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 dal titolare del trattamento. Come specificato dal WP29[120], un *data breach* può essere classificato differentemente in base al fatto che, questa violazione, compromette la riservatezza[121], l'integrità[122] o la disponibilità[123] dei dati personali. In ogni ipotesi, tuttavia, si assiste ad un evento per effetto del quale il Titolare del trattamento non è più in grado di garantire il rispetto dei principi prescritti dall'art. 5 del GDPR. Come precedentemente sottolineato, queste violazioni possono esporre l'interessato a diversi rischi: perdita del controllo dei propri dati personali, furto d'identità, frodi informatiche, lesioni patrimoniali, pregiudizi alla reputazione o alla sfera privata od altri danni materiali, morali o sociale[124].

Proprio in ragione di queste critiche conseguenze, il Legislatore ha predisposto un sistema di notificazione e comunicazione volto a garantire il coordinamento fra il titolare del trattamento, l'autorità nazionale di controllo e, nelle violazioni più gravi, anche dell'interessato.

In particolare, l'art. 33 GDPR delinea il procedimento di notificazione della violazione all'autorità nazionale di controllo, prescrivendo che il titolare del trattamento

---

[118] Cfr. C.C. GIARDINA, *Il Data breach in ambito sanitario: l'importanza di una corretta policy per evitare sanzioni da parte del Garante della Privacy*, in *Azienditalia*, 2021, n. 6, 1067.

[119] Cfr. C. BISTOLFI, *Adozione obbligatoria di strumenti per la sicurezza del trattamento: adozione di specifici strumenti*, in C. BISTOLFI, L. BOLOGNINI, E. PELINO*, Il Regolamento Privacy Europeo,* Milano, 2016, 400-409. Per approfondire v. R. IMPERIALI, *Codice della privacy. Commento alla normativa sulla protezione dei dati personali*, Milano, 2005, 253, ove l'autore sottolinea come se è vero che è impossibile raggiungere una sicurezza in termini assoluti, è necessario quantomeno una tendenza ottimale verso la minimizzazione del rischio.

[120] Cfr. WP29, *Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679, WP250rev.01*, 2018, 8-9.

[121] Cfr. *ibidem*. *s*i ha una violazione della riservatezza quando i dati personali vengono divulgati o siano oggetto di accessi non autorizzati o accidentali.

[122] Cfr. *ibidem*. si ha una violazione dell'integrità dei dati personali quando questi subiscano modifiche non autorizzate o accidentali.

[123] Cfr. *ibidem*. si ha una violazione della disponibilità in caso di perdita, distruzione o accesso accidentale o abusivo ai dati personali.

[124] Cfr. considerando n. 85: "*Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata […]*".

notifichi la violazione all'autorità senza ingiustificato ritardo e, comunque, entro 72 ore da quando venga a conoscenza dalla violazione. Il senso di questo obbligo di notificazione al Garante è da ricondursi ad un generale principio di collaborazione tra Titolare del trattamento e l'autorità di controllo stessa. La reciproca consapevolezza della gravità del *data breach* e la condivisione delle modalità di gestione dello stesso, infatti, consentono ad entrambi di poter adottare, ciascuno per le proprie aree di competenza e ambito operativo, quelle strategie ed ulteriori misure di sicurezza atte a limitare gli effetti e le possibili conseguenze negative della violazione[125].

Ogni *data breach*, chiaramente, rappresenta di per sé un problema, quale indice sintomatico dell'inadeguatezza del regime di sicurezza adottato e, quindi, della vulnerabilità dei dati trattati; tuttavia, il Regolamento non assegna pari importanza ad ogni violazione. Infatti, la procedura di segnalazione all'autorità garante dev'essere attivata solamente quando il titolare valuti che la violazione possa comportare un rischio per i diritti e le libertà dell'interessato [126]. Questa valutazione dovrebbe essere tempestivamente effettuata nel momento in cui il titolare venga a conoscenza della violazione (rappresentando anche il *dies a quo* in base a cui computare le 72 ore per la notifica al Garante) e questi, dovrebbe, in particolare, tener conto della natura e della gravità della violazione, del volume e del tipo dei dati coinvolti (ossia se riguardino categorie particolari di dati), delle sue conseguenze (come la facilità di identificazione degli interessati) e degli effetti negativi per l'interessato (cioè della possibilità che si verifichino le lesioni sopracitate).

Sul punto, è intervenuto anche l'EDPB che, con le Linee guida 01/2021[127], ha descritto alcuni esempi in cui, a seguito di una violazione, fosse opportuno, in ragione dei possibili rischi per l'interessato, notificare il *data breach* all'autorità di controllo competente. Ad esempio, il Comitato ha riconosciuto come, in caso di attacco ransomware al sistema informatico di una piccola impresa, i cui dati siano stati solamente cifrati e non esfiltrati (ossia acquisiti) dall'attaccante, non sia necessario informare l'autorità nazionale di controllo competente, ove i suddetti dati siano stati precedentemente cifrati dal titolare, e la chiave di decifratura non sia stata compromessa, (in modo che l'autore dell'attacco non possa accedere ed utilizzare i dati) e un backup recente dei dati fosse prontamente disponibile (in modo da ripristinare gli stessi in breve tempo). In questo caso, infatti, pur essendoci stato un accesso non autorizzato ai dati e una modifica illecita, la notifica all'autorità di controllo non sarebbe necessaria, data la modesta entità dei dati sottoposti al *data breach*, l'impossibilità

[125] Cfr. *ibidem*, il quale chiarisce che uno degli scopi principali della notifica consiste nel limitare i danni alle persone fisiche.

[126] A precisone di quanto esposto, è necessario sottolineare che il considerando n. 85 collega la procedura di valutazione in esame al principio di *accountability,* escludendo l'obbligo di notifica qualora il titolare "*sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche*". Ciò determina che il titolare si debba dotare di una documentazione adeguata a corroborare, eventualmente in sede di procedimento sanzionatorio, la propria valutazione di non comunicare la violazione all'Autorità. Cfr. C. BISTOLFI, *Principi da osservare*, in C. BISTOLFI, L. BOLOGNINI, E. PELINO (a cura di), *Il Regolamento Privacy Europeo*, Milano, 2016, 336.

[127] Cfr. EDBP, *Linee-guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali*, 2022, in Rete: *https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_it.*

dell'attaccante di avere disponibilità dei dati cifrati e l'assenza di conseguenze sull'operatività del titolare del trattamento che è riuscito, prontamente, a ripristinare i propri sistemi.

Alla luce di quanto sottolineato, ove il titolare, a seguito di un *data breach*, constati un probabile rischio per l'interessato è onerato di notificare la violazione all'autorità di controllo competente. L'art. 33, par. 3, prescrive il contenuto di questa notifica, che può essere sommariamente descritto nella: indicazione della natura della violazione dei dati personali, descrizione della tipologia e portata dei dati violati; comunicazione dei contatti del DPO; descrizione delle probabili conseguenze della violazione; descrizione delle misure di sicurezza già implementate, o in previsione di essere implementate, per porre rimedio alla violazione dei dati personali e eventualmente attenuarne i possibili effetti negativi.

Parallelamente a quanto previsto dalla norma precedente, l'art. 34 GDPR è dedicato alla comunicazione della violazione all'interessato. Lo scopo di questa comunicazione è quello di consentire all'interessato, i cui dati sono stati coinvolti nel *data breach,* di mettere in atto nel più breve tempo possibile le contromisure volte a proteggersi dalla violazione e/o a limitare il danno[128].

Anche la comunicazione all'interessato presuppone che il titolare faccia una valutazione sulla sussistenza, a seguito della violazione, di rischi elevati per i diritti e le libertà dell'interessato stesso. Il riferimento al 'rischio elevato' mostra come il Legislatore comunitario abbia modulato i differenti obblighi cui è tenuto il titolare collegandoli a crescenti livelli di gravità del rischio atteso.

La necessità di comunicazione con l'interessato, infatti, può rappresentare un grande peso – soprattutto in termini reputazionali – per il titolare del trattamento, il quale, sostanzialmente, dovrà direttamente ammettere i propri errori nella gestione della sicurezza dei dati personali affidati dagli interessati, per lo svolgimento del suo trattamento. Per questo motivo, proprio per evitare pratiche fugaci, volte, sostanzialmente, a 'salvare la faccia' del titolare, è previsto che la comunicazione del *data breach* all'interessato avvenga in linea con il principio di trasparenza e correttezza, garantendo informazioni chiara e precisa sulla natura, portata e possibili conseguenze della violazione[129].

Infine, a conclusione dell'art. 33 GDPR, la normativa prevede che il titolare del trattamento sia tenuto a documentare tutte le violazioni dei dati personali. Quest'obbligo è direttamente connesso al principio di *accountability,* con lo scopo di permettere all'Autorità di effettuare eventuali verifiche sul rispetto delle norme. Come suggerito dal WP29, tale obbligo può essere assolto con l'istituzione di un apposito registro, nel quale inserire le informazioni riguardati ciascuna violazione, comprese quelle che il titolare ha ritenuto di non dover notificare all'autorità[130].

---

[128] Cfr. M. MASSIMI, *Articolo 34 – Comunicazione di una violazione dei dati personali all'interessato*, in E. BELISARIO, G.M. RICCIO, G. SCOZZA (a cura di), *GDPR e Normativa Privacy*, Milano, 2020, 401-407.

[129] Cfr. E. PELINO*, Adempimenti per violazioni dei dati personali (c.d. data breach)*, in C. BISTOLFI, L. BOLOGNINI, E. PELINO, *Il Regolamento Privacy Europeo*, Milano, 2016, 451-452.

[130] Cfr. EDPB, *Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679*, *op. cit.*, 26-27, ove si espongono le linee operative di tenuta e conservazione del registro dei *data breach.*

4.5 Il Modello Organizzativo Privacy

Nella predisposizione di misure organizzative utili a soddisfare il principio di *accountability,* soprattutto in relazione agli adempimenti documentali necessari per dimostrare la *compliance* agli obblighi normativi, nella prassi [131] si è sviluppato il fenomeno di raggruppare tali misure in uno specifico modello organizzativo. Il MOP (acronimo di Modello Organizzativo Privacy) rappresenta, quindi, uno strumento pratico che consente al titolare del trattamento di raggruppare in modo organico e compatto l'insieme delle regole e procedure predisposte nella propria organizzazione per far fronte agli adempimenti previsti in materia di protezione dei dati personali.

Il MOP non rientra tra gli adempimenti obbligatori previsti dal Regolamento. La sua adozione, pertanto, è puramente opportuna e legata alla volontà (o più spesso necessità) di adottare misure organizzative rivolte a garantire l'adeguamento dell'organizzazione del titolare al GDPR.

La valutazione dell'opportunità di adottare tale modello è legata, come anche altre misure previste dal Legislatore europeo, ad una serie di criteri. In particolare, oltre al criterio dimensionale o dei costi di attuazione per l'organizzazione [132], il titolare dovrebbe tener conto del settore (e quindi del contesto) in cui la propria organizzazione opera, della quantità di interessati oggetto del trattamento e dei dati personali trattati, della tipologia di dati, della natura, portata e modalità del trattamento e, infine, dei rischi che il trattamento può presentare sugli interessati. A fronte di tali considerazioni, pertanto, sarebbe opportuno che il titolare si doti di questo strumento organizzativo ove operi in un contesto operativo caratterizzato da ingenti dati e innumerevoli trattamenti svolti, cioè, in generale, in presenza di scenari ad alto impatto privacy[133].

L'origine di questo strumento organizzativo deriva principalmente dal Documento Programmatico sulla Sicurezza previsto dalla l. 675/1996, e successivamente dal d.lgs. 196/2003 (Codice Privacy), ove il suo scopo era quello di contenere un insieme di regole che, se adempiute, consentivano il corretto adempimento della previgente disciplina sulla protezione dei dati personali. Successivamente all'entrata in vigore del GDPR, e all'abrogazione di gran parte del Codice Privacy, il MOP ha acquisito una serie di caratteristiche tipiche del modello organizzativo di gestione previsto dal d.lgs. 231/2001 in tema di responsabilità amministrativa degli enti giuridici. Un Modello Organizzativo e di Gestione ai sensi del d.lgs. 231/2001 è un insieme di protocolli, che regolano e definiscono la struttura aziendale e la gestione dei suoi processi sensibili. Giova evidenziare che lo scopo ultimo dei modelli organizzativi 231 è quello di ridurre il rischio di commissione di illeciti penali all'interno dell'organizzazione dell'impresa, esimendo,

[131] È da evidenziare che la necessità di sviluppare modelli di razionalizzazione degli adempimenti connessi alla protezione dei dati personali non si è sviluppato solo nell'ambito delle organizzazioni private ma anche negli enti pubblici, a fronte della portata e natura dei trattamenti da questi svolti. Cfr. A. MONEA, *Regolamento n. 2016/679: la necessità di uno specifico "Modello organizzativo" per la protezione dei dati personali,* in *Azienditalia*, 2019, n. 8-9, 1114-1123.

[132] Anche se è da evidenziare che i predetti criteri possono essere particolarmente ingannevoli, in quanto non sempre le dimensioni di un'organizzazione corrispondono ad una maggiore complessità di tipo organizzativo o ad un impatto sulla gestione dei dati personali rilevante.

[133] Cfr. M. PEREGO, S. PERSI, C. PONTI, *Il Modello Organizzativo Privacy – MOP*, Torino, 2020, 21-22.

in questo modo, l'ente giuridico da ogni responsabilità per i reati commessi da persone fisiche ad essa collegate.

Su questo punto insiste anche il MOP[134]. Pur essendo assolutamente assente nel Regolamento una qualsiasi clausola di esenzione da responsabilità per titolari o responsabili del trattamento, come ogni misura di *accountability* documentabile, il MOP permette di dar prova della corretta gestione dei dati in coerenza con i flussi organizzativi della struttura del titolare. In questo modo, ove il titolare abbia adottato ed efficacemente attuato un MOP all'interno della propria organizzazione, è facile pensare che questo gli comporti diversi vantaggi in termini probatori, ove venga contestata la liceità del suo trattamento. Se quanto detto può essere valutato come il vantaggio nell'adozione di un MOP, la prassi riconosce allo stesso un ulteriore finalità. In particolare, il MOP servirebbe a condensare in un unico testo una serie di documenti e protocolli che, in assenza, sarebbe complicato gestire, specialmente in realtà medio-alte complesse. La ragione di questa razionalizzazione dei flussi documentali amministrativi può essere rinvenuta anche in relazione ad un principio fondamentale ella documentazione sui sistemi di gestione, il quale richiede che non si duplichi mai un testo o di parte di un testo in documenti differenti.

Così come per i modelli organizzativi del d.lgs. 231/01, anche per la gestione dei dati personali il modello organizzativo dev'essere adattato alle varie realtà organizzative dei titolari del trattamento, rendendo impossibile la creazione di uno *standard* unitario. Infatti, oltre a tener conto dell'organizzazione del titolare, il MOP dev'essere realizzato (o aggiornato se già esistente) ogni qual volta vi siano dei mutamenti di contesto al trattamento, interni o esterni all'organizzazione del titolare[135]. D'altronde, dato che il MOP contiene quelle regole e procedure volte a garantire una corretta gestione del trattamento, si rende necessario il suo costante aggiornamento a frequenza del verificarsi di un evento modificativo del trattamento, al fine di adeguare la singola documentazione in esso raggruppata[136].

Data l'assenza nel Regolamento di qualunque indicazione sui possibili contenuti del MOP, per strutturare tale modello si è ritenuto dover partire, in primo luogo, dal considerando n. 74[137] e dall'art. 24 GDPR[138] quali clausole generali disciplinanti l'obbligo di *accountability*. Anche l'art. 25 GDPR potrebbe essere considerato come aggancio normativo per il MOP, quale misura organizzativa per realizzare il principio della *privacy by design* e *by default,* garantendo, cioè, sin dalla progettazione dell'organizzazione del titolare del trattamento, misure adeguate a garantire i dati personali. Partendo da tali presupposti, quindi, sarebbe corretto ritenere che tutte le disposizioni del Regolamento,

[134] Cfr. *ivi*, 5-10.

[135] A titolo esemplificativo, ove muti il contesto, la portata o la natura dei dati trattati, la finalità del trattamento, le misure di sicurezza disponibili o i rischi connessi ai diritti e libertà dell'interessato.

[136] A questo proposito, è da riferente necessaria anche una revisione periodica del Modello, al fine di adeguare la documentazione e le misure intraprese all'evoluzione tecnologica.

[137] Cfr. M. PEREGO, S. PERSI, C. PONTI, *op. cit.*, 22-23. In particolare, le misure dovrebbero essere efficaci nel dimostrare che la loro applicazione permette il raggiungimento degli obiettivi di tutela previsti nel regolamento.

[138] Cfr. *ibidem.* Da questo punto di vista, il MOP rappresenterebbe l'insieme delle specifiche misure tecniche e organizzative adeguate, comprese l'attuazione di politiche adeguate in materia di protezione dei dati, volte a dimostrare che i trattamenti effettuati dall'organizzazione siano conformi al Regolamento.

le quali risultino declinazione del principio di *accountability,* possano fornire un loro apporto per identificare i contenuti, almeno di base, del modello. A tal fine, sarebbe opportuno inserire all'interno del MOP: il registro dei trattamenti (art. 28 GDPR); un analisi dei rischi e della metodologia utilizzata per la valutazione dei rischi (art. 35 GDPR); delle misure e procedure di mitigazione rivolte a prevenire il rischio di *data breach* (art. 32 GDPR); della predisposizione di una procedura per la gestione della *data retention*; dei modelli di documenti (informativa per i vari tipi di interessati, atto di designazione del responsabile e dell'autorizzato al trattamento, i contratti di responsabilità e quelli di contitolarità e, in generale, ogni altro documento ritenuto necessario per l'organizzazione) [139] .In questo modo, attraverso il modello, sarebbe possibile sistematizzare, in modo organico, tutta la documentazione delle procedure e misure adottate nel corso del processo di adeguamento al GDPR[140].

Questo insieme di documenti, tuttavia, rappresenta solo una parte o 'fase' del MOP. Infatti, come riconosciuto dalla prassi[141], il modello si compone, dal punto di vista operativo, da due parti principali:

1. la prima è definita come parte, o 'fase', statica e conterrebbe tutti i documenti precedentemente elencati, i quali rappresenterebbero l'iter che l'organizzazione del titolare ha seguito per adeguarsi alla disciplina del Regolamento;
2. la seconda, invece, è la parte, o 'fase', dinamica del modello, cioè quella rivolta al progressivo e costante aggiornamento del documento stesso.

Quest'ultimo rappresenta propri il punto nodale di questo strumento. Seguendo, infatti, la logica propria del *Ciclo di Deming: Plan-Do-Check-Act (PDCA)* [142] , il MOP

[139] Cfr. M. PEREGO, *MOP: il Modello Organizzativo Privacy come misura di accountability per la compliance al Gdpr,* in *Federprivacy,* 2022, in Rete: *https://www.federprivacy.org/informazione/primo-piano/mop-il-modello-organizzativo-privacy-come-misura-di-accountability*.

[140] Cfr. *ibidem*. In particolare, l'autrice sottolinea come, per aumentare il valore del MOP in termini di *accountability*, potrebbero essere inseriti quali contenuti ulteriori: l'organigramma privacy ed il mansionario per le risorse che rivestono specifiche responsabilità in materia di protezione dei dati (i quali permettono di inquadrare correttamente, in una determinata struttura, tutti i soggetti interni ed esterni che trattano i dati personali con la precisa indicazione dei flussi di dati intercorrenti); lo scadenziario; il piano di formazione per il personale; il piano di audit; lo stato di presa in carico delle criticità precedentemente rilevate a seguito di *data breach*, *audit*, reclami e segnalazioni; le motivazioni alla base delle scelte relative ai trattamenti effettuati; indicatori afferenti alla protezione dei dati che permettono di comprendere, tramite dati oggettivi e riproducibili, l'efficacia e l'efficienza delle misure poste in atto per la mitigazione dei rischi.

[141] Cfr. M. PEREGO, S. PERSI, C. PONTI, *op. cit.*, 9-10; R. CASTROREALE, C. PONTI, *Il sistema integrato per la sicurezza delle informazioni ed il GDPR: guida operativa all'efficace integrazione dei due mondi anche con l'ausilio della ISO/IEC 27701*, Roma, 2021, 231-234.

[142] Il ciclo di Deming (o ciclo di PDCA, acronimo dall'inglese *Plan–Do–Check–Act*) è un metodo di gestione iterativo per il controllo e il miglioramento continuo dei processi e prodotti. Adattando il ciclo nell'ambito *data protection,* nel dettaglio, si può fare riferimento agli elementi del PDCA come:

- *Plan:* pianificazione delle attività da svolgere per assicurare la protezione dei dati personali;
- *Do*: analisi di tutti i processi dell'organizzazione per garantire che i principi di *privacy by design* e *by default*, nonché gli obblighi previsti in tema di diritti, sicurezza, violazione, conservazione e portabilità dei dati, siano adeguatamente documentati;
- *Check*: sperimentazione del modello e verifica dell'efficacia dello stesso;
- *Act*: fase finale relativa alla standardizzazione e al miglioramento dei processi relativi al trattamento, avviata una volta che il primo blocco di controlli abbia dato esito positivo.

rappresenterebbe un vero e proprio organismo che muterebbe ed evolverebbe nel tempo, affrontando i cambiamenti, interni od esterni, che possono occasionarsi nell'organizzazione del titolare del trattamento, garantendo l'adeguamento di tutti i flussi operativi dell'organizzazione ai principi del GDPR, in modo da rendere l'organizzazione del titolare *compliant.*

Come sopra specificato, i modelli organizzativi nascono con la finalità di condensare tutte le procedure e la documentazione ad esse allegate, in un unico strumento, al fine di garantire un'agevole verifica, aggiornamento e uso dei propri contenuti. Appare, quindi, di preminente importanza la necessità di includere il MOP all'interno di un contesto integrato agli altri modelli di organizzazione della *compliance* degli enti e imprese. In un sistema normativo caratterizzato da una notevole *impasse* normativa sull'attività imprenditoriale, l'utilità dei modelli organizzativi si rinviene anche nella possibilità degli stessi di interfacciarsi o, in alcuni casi, integrarsi a vicenda.

Nel nostro ordinamento vi sono diversi esempi che possono essere tratti per evidenziare la possibilità di integrazione fra i modelli organizzativi predisposti dalle imprese e le norme su cui questi si fondano. Uno fra questi è dato dal rapporto fra il MOP e il modello dettato dal d.lgs. 231/2001 in materia di responsabilità amministrativa degli enti. Come previamente richiamato, infatti, tra le misure che l'ente giuridico può adottare per adeguarsi al d.lgs. 231/2001 vi è la stesura del Modello di Organizzazione e di Gestione (c.d. MOG), il quale presenta e condivide con il MOP diversi punti di contatto e prassi operative:

- individuare le attività di trattamento di dati personali sensibili e/o più a rischio di violazioni e procedere a una valutazione di impatto sul trattamento dei dati quando un trattamento presenta rischi elevati per i diritti e le libertà delle persone fisiche (art. 35 GDPR) e parallelamente, individuare le attività nel cui ambito possono essere commessi reati (art. 6, co. 2, lett. a), d.lgs. 231/2001);
- svolgere attività di formazione del personale per assicurare che coloro i quali agiscono per conto del titolare (o del responsabile) siano adeguatamente istruiti e formati sulla normativa vigente in materia di privacy (artt. 29 e 32, par. 4, GDPR) e in relazione ai modelli di prevenzione dai reati (art. 6, co. 2, lett. b)-d), d.lgs. 231/2001);
- implementare misure tecniche e organizzative adeguate ad assicurare, sia l'attuazione dei principi della privacy by design e by default, sia un livello di sicurezza adeguato al rischio (artt. 25 e 32 GDPR). Nell'ambito del d.lgs. 231/2001 il riferimento all'art. 6, co. 2, lett. c), è più ampio, comprendendo ogni modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- una volta scoperto un *data breach*, adottare, anche successivamente ad esso, misure idonee a scongiurare un rischio elevato per i diritti e le libertà degli interessati, rivedendo e aggiornando costantemente le misure adottate (art. 34 GDPR). Parallelamente, si prevede la verifica e modifica del modello organizzativo 231 ove venga scoperta una violazione delle prescrizioni in esse contenute, e quindi venga commesso un reato (art. 7, co. 4, 1° periodo, d.lgs. 231/2001);

Per approfondire, v. N. BERNARDI (a cura di), *Privacy. Protezione e trattamenti dei dati,* IPSOA Manuali, Milano, 2019, 489-490.

- procedere a riesame della valutazione d'impatto sulla protezione dei dati quando insorgono variazioni del rischio nelle attività di trattamento (art. 35 GDPR) e, parallelamente, riesaminare il modello di rischio contenuto nel MOG ove avvengano mutamenti nell'organizzazione o nell'attività (art. 7, co. 4, 2° periodo, d.lgs. 231/2001). In entrambe le circostanze, il riesame degli strumenti è volto ad aggiornare le misure tecniche ed organizzative necessarie per soddisfare i requisiti della protezione dei dati personali e della prevenzione dei reati nell'organizzazione del titolare del trattamento[143].

Ulteriormente al rapporto fra il MOP e il Modello organizzativo ai fini della 231/2001, altri esempi di integrazione fra modelli organizzativi diversi sono: tra il MOP e la normativa *Whistelblowing*[144], tra il MOP e la normativa in tema di trasparenza e diritto di accesso nei confronti della Pubblica Amministrazione[145], tra il MOP e la disciplina a tutela del consumatore[146] e tra il MOP e le norme ISO/IEC in materia di Sicurezza delle informazioni.

5 Certificazioni: definizioni, scopo e vantaggi

Nell'epoca della globalizzazione si è assistito al fenomeno per cui, affianco a regole e modelli legislativamente imposti si sono posizionate altre regole, spesso fondate proprio su quelle legislative, che i soggetti privati si sono autoimposti per regolare le proprie attività. Il fenomeno dell'autoregolamentazione dei privati, inserendosi nel più ampio contesto dello sviluppo della *soft law* e della co-regolamentazione[147], consiste nella possibilità lasciata agli operatori economici, alle parti sociali, alle organizzazioni non governative, o alle associazioni, di adottare tra di loro e per sé stessi orientamenti comuni, non presupponendo una presa di posizione da parte delle istituzioni[148]. Questo fenomeno è strettamente collegato al diritto, in quanto è lo stesso ordinamento che ammette la creazione di regole al di fuori delle fonti istituzionali. Il vantaggio dell'autoregolamentazione è che questa garantisce la possibilità di specificare e rendere maggiormente 'concrete' le sempre più frequenti norme di principio che vengono

[143] Cfr. G. RIZZINI, *I nodi tra privacy e responsabilità 231 nei rapporti tra soggetti pubblici e privati,* in *Il Quotidiano Giuridico*, 2023, in Rete: *https://www.altalex.com/documents/2023/02/08/nodi-privacy-responsabilita-231-rapporti-soggetti-pubblici-privati*; M. PEREGO, S. PERSI, C. PONTI, *op. cit.*, 56-60.

[144] In particolare, il d.lgs. 24/2023 attuativo della Direttiva *Whistleblowing*, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e nazionale che ledono l'interesse pubblico o l'integrità della pubblica amministrazione o dell'ente privato, di cui sono venuti a conoscenza nel contesto lavorativo.

[145] Nello specifico, il Decreto Trasparenza (d.lgs. 33/2013), in relazione alla gestione dell'accesso civico generalizzato e gli artt. 22 e *ss*. della l. 241/1990 in relazione al diritto di accesso agli atti.

[146] Il rapporto fra il Regolamento (UE) 2016/679 e la disciplina a protezione dei consumatori è stato rafforzato dalla Direttiva (UE) 2019/2161 "Omnibus", recepita in Italia con il d.lgs. 26/2023, la quale prevede delle tutele specifiche a fronte dell'acquisto di servizi, da parte dei consumatori, con i propri dati personali. Sul punto, v. L. CAPPELLO, *L'evoluzione del consumatore negli ecosistemi decentralizzati: l'impatto della digitalizzazione e della blockchain*, Torino, 2022.

[147] Cfr. A.R. POPOLI, *Codici di condotta e certificazioni*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, 367-373.

[148] Cfr. PARLAMENTO EUROPEO, CONSIGLIO EUROPEO, COMMISSIONE EUROPEA, *Progetto Interistituzionale - «Legiferare meglio», G.U. 2003/C 321/01,* 2003, punto 22.

legislativamente adottate. La necessità del Legislatore di produrre norme di portata generale e con una bassa obsolescenza è, quindi, bilanciata dalla possibilità della prassi di autoregolamentarsi. Ciò permetterebbe certamente una regolamentazione più celere e semplice che, sulla base dei principi legislativamente previsti, permetterebbe di avere delle norme adeguate e immediatamente applicabili ai problemi e necessità della prassi, mantenendo, comunque, un raffronto e controllo pubblicistico.

Rispetto a quanto sopra premesso, le certificazioni, insieme ai codici deontologici (o di condotta), rappresentano una fra le principali forme di autoregolamentazione dei privati. In particolare, le certificazioni costituiscono un modello regolatorio privatistico che permette di fissare *standard* comuni a cui tutti i soggetti interessati devono conformarsi per poter ottenere un certo *status*.

Analizzando ulteriormente l'oggetto, in dottrina si sostiene che l'attività di certificazione consiste nella valutazione, verifica ed attestazione, da parte di un soggetto terzo, imparziale ed indipendente (c.d. organismo di certificazione), della conformità a determinati parametri di un prodotto o un servizio, di un sistema produttivo o del personale di una determinata impresa od organizzazione[149]. Come sovra evidenziato, la conclusione positiva di questo procedimento determina il rilascio di un'attestazione e della licenza di utilizzo di un dato marchio, che sottolinea direttamente a terzi la conformità dell'entità certificata con un determinato sistema di norme.

A fronte di ciò, le certificazioni, oltre ad essere uno strumento per misurarne l'osservanza di un determinato insieme di regole, rappresenterebbero anche un importante metodo di *marketing*., permettendo al soggetto certificato di raggiungere nuovi *stakeholders*. In questo modo, le certificazioni possono essere un elemento utile per aumentare, soprattutto, il livello reputazionale e la notorietà delle imprese su determinati settori del mercato caratterizzati da un'alta competitività, 'attirando' i soggetti che sono alla ricerca di un bene o servizio. La reputazione, infatti, utilizzando una nozione civilista, altro non è che la rappresentazione della personalità di un soggetto in una cerchia di consociati. La reputazione è l'opinione che i terzi hanno del valore di un soggetto; è la percezione esteriore dell'immagine di un ente collettivo[150]. La reputazione, al pari degli altri diritti della personalità, si inquadra nel sistema di diritti costituzionalmente garantiti, la cui tutela emerge principalmente dagli artt. 2 e 3 Cost., quali fattispecie aperte volte a proteggere la persona integralmente, in tutti i suoi modi di essere e verso tutti i consociati. Ciò è pacificamente riconosciuto anche dalla Consulta e dalla Corte di Cassazione, le quali hanno identificato come nella sfera dei diritti della personalità umana, esiste un vero e proprio diritto soggettivo perfetto alla reputazione personale anche al di fuori delle ipotesi espressamente previste dalla legge ordinaria (e

[149] Cfr. A.R. POPOLI, *Codici di condotta e certificazioni, op.cit.*367-373; E. BELLISARIO, *Certificazioni di qualità e responsabilità civile*, Milano, 2011, 11. Sul punto, il riferimento normativo principale è dato dalla norma ISO/IEC 17000:2020, la quale, al punto 7.6, definisce la certificazione come "*una attestazione rilasciata da una parte terza (organismo di certificazione - OdC) relativa a un oggetto (prodotto, processo, servizio, persona o sistema) sottoposto a valutazione della conformità rispetto a requisiti contenuti in una norma tecnica (standard) o in un disciplinare specifico*".

[150] Sul tema della reputazione nel contesto imprenditoriale v. A. BARCHIESI, S. PREVITI, F. SANZARI (a cura di), *Web reputation e identità aziendale online: strumenti di tutela*, Milano, 2019, 5-29.

in particolare dalle norme penali), che va inquadrato nel sistema di tutela costituzionale della persona umana, traendo nella Costituzione il suo fondamento normativo[151].

Le certificazioni, però, al più che accrescere il livello reputazionale dei singoli individui, coinvolgono principalmente gli imprenditori nella forma di enti collettivi, e quindi persone giuridiche. In considerazione di questi soggetti, il concetto di reputazione può essere inteso come "*fusione di tutte le aspettative, percezioni ed opinioni sviluppate nel tempo da clienti, impiegati, fornitori, investitori e vasto pubblico in relazione alle qualità dell'organizzazione, alle caratteristiche e ai comportamenti, che derivano dalla personale esperienza, il sentito dire o l'osservanza delle passate azioni dell'organizzazione*" [152] . Anche questo concetto di reputazione risulta essere costituzionalmente tutelata sempre dal medesimo art. 2 Cost, il quale, prevedendo che la Repubblica riconosce e garantisce i diritti inviolabili dell'uomo sia come singolo sia nelle forme sociali, va a riconoscere una serie di diritti della personalità a tutte le estrinsecazioni sociali dei singoli, fra cui anche gli enti collettivi (e imprenditoriali ai fini di questa trattazione)[153].

Perciò, anche attraverso una tale protezione, risulta evidente come le imprese cerchino di aumentare la propria reputazione attraverso il circuito delle certificazioni, rappresentando, queste ultime, un ottimo strumento per porsi in luce in un contesto imprenditoriale fitto e competitivo. In questo modo, la presenza di un attestato certificatorio, rilasciato da un soggetto terzo e imparziale, si tradurrebbe una maggiore percezione morale da parte degli *stakeholders,* garantendo indubbi vantaggi in termini di competitività e presenza sul mercato.

Dal punto di vista organizzativo, inoltre, le certificazioni permettono di razionalizzare costi e rischi (sanzionatori e reputazionali), in relazione all'adeguamento delle imprese alla legislazione europea inerente al Mercato Unico Europeo. Rientrando il GDPR all'interno di questo settore, e in particolare all'interno del Mercato Unico Digitale, l'introduzione di certificazioni sulla *compliance* alla protezione dei dati personali rappresenta una spinta in più per realizzare un sistema di gestione della protezione dei dati personali efficace (in linea, quindi, con i modelli organizzativi adeguati richiesti dalla normativa europea), anche se attuata con modelli privatistici. Tali certificazioni permetterebbero ai titolari e responsabili dei trattamenti di comprovare l'effettivo rispetto della normativa inerente alla protezione dei dati personali e,

---

[151] Cfr. V. SPINA, L'azione di risarcimento dei danni da diffamazione, in *Altalex*, 2021, in Rete: *https://www.altalex.com/guide/azione-di-risarcimento-danni-da-diffamazione*. In particolare, tale diritto trarrebbe fondamento dagli artt. 2 e 3 Cost (*ex plurimis* Corte cost., 14/07/1986, n. 184 e Corte cost., 30/07/2021, n. 178, in *One Legale*). Inoltre, l'a. sottolinea come "*nell'ambito dei diritti della personalità umana, il diritto all'immagine, al nome, all'onore, alla reputazione, alla riservatezza non sono che singoli aspetti della rilevanza costituzionale che la persona, nella sua unitarietà, ha acquistato nel sistema della Costituzione. Trattasi quindi di diritti omogenei, essendo unico il bene protetto (Cassazione Civile, sez. III, 10 maggio 2001, n. 6507*, in *One Legale)*".

[152] Cfr. R. BENNETT, R. KOTTASZ, *Practitioner perceptions of corporate reputation: an empirical investigation*, in *Corporate Communications: An International Journal*, 2000, vol. 5, n.4, 224-234.

[153] Tale assetto è ormai consolidato nella giurisprudenza di legittimità, la quale, in numerose sentenze va a riconoscere che anche le persone giuridiche, ed in genere agli enti collettivi, godano di situazioni giuridiche equivalenti ai diritti fondamentali della persona umana costituzionalmente protetti, quale il diritto all'immagine e alla reputazione, *ex pluris* Cass. civ., Sez. III, 4 giugno 2007, n. 12929; Cass. civ., Sez. lavoro, 1° ottobre 2013, n. 22396; Cass. civ., Sez. I, 25 luglio 2013, n. 18082, in *One LEGALE*.

conseguentemente, mettersi al riparo da possibili sanzioni. Sotto questo profilo, come sottolineato nei precedenti capitoli, il sistema di gestione della privacy si porrebbe come strumento analogo ai Modelli di organizzazione e gestione di cui al d.lgs. 231/2001, consentendo al titolare del trattamento, tutte le volte in cui dimostri di aver adottato e correttamente applicato un sistema o modello organizzativo per la gestione dei propri trattamenti, un'esenzione, o comunque una sottodimensione, da ogni responsabilità per eventuali trattamenti illeciti che siano frutto di circostanze non controllabili dal titolare stesso. D'altronde è proprio l'art. 24 GDPR ad indicare come i titolari possano fornirsi di certificazioni ai fini della dimostrazione della propria *compliance* al regolamento e che questo, pur non esimendo da responsabilità, garantisce una presunzione relativa di conformità del trattamento di dati effettuato dal titolare, liberamente valutabile del Garante in sede di controllo e, soprattutto, in termini sanzionatori.

In conclusione, riassumendo quanto esposto, le certificazioni permettono, al soggetto certificato, di dimostrare, al mercato o alle autorità, la capacità di:

1. strutturarsi e gestire le proprie risorse e i propri processi produttivi in modo tale da riconoscere e soddisfare i requisiti legislativamente previsti per una data attività, nonché l'impegno a migliorare continuamente questa capacità;
2. ottenere e mantenere la conformità dei prodotti realizzati o dei servizi erogati. A fronte di ciò, l'organizzazione può ottenere un marchio che evidenzi ai terzi la conformità del prodotto o servizio certificato;
3. possedere, e mantenere nel tempo, le abilità, le conoscenze e le competenze (tecniche ed organizzative) richieste per lo svolgimento di determinate attività imprenditoriali.

Con la conseguenza finale che, i soggetti che ricorrono alla certificazione ottengono notevoli vantaggi in termini di una maggiore efficienza e competitività, anche grazie a un incremento della fiducia nella qualità dei servizi che offrono sul mercato.

6 Schemi di certificazione ISO in materia di sicurezza e protezione delle informazioni

Prima di procedere all'analisi della disciplina prevista dal Regolamento in tema di certificazioni è preliminarmente necessario esporre una disamina, seppur sommaria, sui principali schemi di certificazione pubblicati dall'Organizzazione Internazionale per la Normazione (ISO) in tema di sicurezza delle informazioni, *cybersecurity* e protezione della privacy.

L'ISO è un'organizzazione internazionale indipendente che svolge attività consultive per l'ONU e l'UNESCO in tema di normazione tecnica ed è costituita dagli organismi nazionali di standardizzazione dei 164 paesi aderenti[154]. Scopo dell'ISO, e degli

[154] Per l'Italia è l'Ente nazionale italiano di unificazione, "UNI" nella sigla che identifica gli standard, è l'associazione privata, senza finalità di lucro, di riferimento a livello nazionale per la produzione ed armonizzazione delle norme volontarie tecniche in tutti i principali settori, escluso quello elettrico ed elettrotecnico. UNI, è il soggetto che rappresenta l'Italia presso l'ISO e le Organizzazioni sovranazionali di normazione. Gli altri enti di standardizzazione di riferimento a livello internazionale ed europeo sono l'*International Electrotechnical Commission* (IEC) e il Comitato di normazione europeo (CEN), anche quest'ultimo facente parte dell'ISO.

altri enti ad esso aderenti, è quello di favorire "*il libero scambio, garantire la salute e sicurezza dei lavoratori e dei consumatori e proteggere l'ambiente"*[155], attraverso la standardizzazione dei settori dell'economia, a livello internazionale, europeo o nazionale, mediante la creazione di regole tecniche e disciplinari che vengono, poi, condensati e sviluppati in schemi di certificazione. Le certificazioni e le linee guida adottate dall'ISO sono di carattere volontario; pertanto, l'adesione ad esse non è obbligatoria per legge, ma, data l'autorevolezza dell'organizzazione, i suoi standard sono altamente accreditati nel contesto imprenditoriale.

Lo sviluppo delle regole tecniche dell'ISO è avvenuto anche in tematiche inerenti alla *data protection.* Da tempo, infatti, sono disponibili diversi standard tecnici in tema di sicurezza delle informazioni, sistemi di gestione delle informazioni sensibili e servizi *cloud*. Sin dalla Direttiva Madre, questi costituivano i principali meccanismi di certificazione in tema di protezione dei dati. Tuttavia, a fronte dei risultati ottenuti durante la vigenza della precedente normativa, nel corso del dibattito parlamentare europeo per la formazione del GDPR, il Legislatore europeo ha compreso l'importanza di dotarsi di nuovi strumenti, fra cui certificazioni e codici di condotta, non più basati sulle norme ISO all'epoca esistenti, bensì sui principi e sui concetti del futuro Regolamento in materia di protezione dei dati personali[156].

La necessità di discostarsi dagli standard tecnici ISO è data, principalmente, dal fatto che queste ultime si concentrano sulla protezione e sulla sicurezza delle organizzazioni, e dei loro dati e informazioni, nei confronti di eventuali minacce, quando il fulcro del GDPR è rivolto alla protezione dei diritti fondamentali delle persone fisiche attraverso il diritto al controllo dei propri dati. Questo ha portato il Legislatore ad elaborare un nuovo modello legislativo di certificazione rivolto a scopi diversi rispetto alle norme tecniche ISO. Ciononostante, non si può non sottolineare che ove si aderisca alle diverse certificazioni ISO, riguardanti regole tecniche in tema di cybersicurezza e gestione delle informazioni, vengono sicuramente soddisfatti parte dei requisiti e principi previsti dal GDPR.

Questa differenza di prospettiva è apprezzabile anche in relazione ai principali schemi di certificazione ISO attualmente esistenti.

6.1 Serie ISO/IEC 27000: Information Security Management Systems (ISMS) Family of Standards

La serie di standard ISO/IEC 27000 raggruppa insieme di norme tecniche rivolte a disciplinare i sistemi di gestione per la sicurezza delle informazioni implementabili dalle

[155] V. anche il sito web ufficiale dell'ISO, in Rete: *https://www.iso.org/about-us.html.*

[156] Cfr. considerando n. 100: "*Al fine di migliorare la trasparenza e il rispetto del presente regolamento dovrebbe essere incoraggiata l'istituzione di meccanismi di certificazione e sigilli nonché marchi di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi*".

organizzazioni per progettare i propri dati finanziari, informazioni strategiche, know-how e proprietà intellettuali, nonché i dati dei dipendenti, clienti e terzi[157].

In particolare, la norma tecnica che contiene i requisiti per la l'implementazione, il mantenimento e il miglioramento di un sistema di gestione della sicurezza delle informazioni è la ISO/IEC 27001.

Questa norma presenta diversi punti in comune con il GDPR. Se, in generale, il Regolamento non riporta delle misure minime di sicurezza da adottare, lasciando il compito ai titolari del trattamento di individuare quelle più adeguate, in relazione al rischio del trattamento, con lo standard ISO/IEC 27001:2013 viene prevista una lista di controlli di sicurezza che permetterebbero al titolare del trattamento (e all'*auditor*) di valutare l'adeguatezza delle misure adottate o, eventualmente, di metterne in atto ulteriori.

Altro punto di contatto fra lo standard e il Regolamento è dato dall'analisi dei rischi che possono compromettere la sicurezza delle informazioni. Infatti, come il GDPR, lo schema ISO/IEC 27001 concentra la propria valutazione analisi-rischi sul mantenimento della riservatezza, integrità e disponibilità delle informazioni e, in caso di perdita di queste condizioni, considera gli impatti e le conseguenze che la violazione possa avere sull'organizzazione[158].

Infine, a partire dalla ISO/IEC 27001:2022[159] e ISO/IEC 27701:2019[160], si rileva una maggiore attenzione, della serie ISO/IEC 27000, anche ai dati personali delle persone fisiche. Infatti, si prevedono ulteriori requisiti inerenti all'implementazione di un sistema di gestione della privacy, estendendo l'applicazione delle norme in questione anche alla sicurezza dei dati personali. In questo modo vengono inclusi, tra gli elementi interessati al sistema di gestione della riservatezza, anche le persone fisiche i cui dati sono oggetto del trattamento, e non solo i dati 'sensibili' dell'organizzazione; con la conseguenza che saranno ampliati gli *audit* di verifica del sistema anche in relazione al ruolo proprio

---

[157] Cfr. UNI, *Una terminologia comune per la sicurezza delle informazioni*, 2016, in Rete: *https://www.uni.com/index.php?option=com_content&view=article&id=4686:una-terminologia-comune-per-la-sicurezza-delle-informazioni&catid=171:istituzionale&Itemid=2612#.*

[158] La coerenza della regola ISO/IEC 27001 rispetto al GDPR è data anche dall'implementazione del controllo A.16.1 (Gestione degli incidenti relativi alla sicurezza delle informazioni e dei miglioramenti), il quale, similmente all'art. 32 GDPR, dovrebbe assicurare "*un approccio coerente ed efficace alla gestione degli incidenti in materia di sicurezza informatica, compresa la comunicazione sugli eventi di sicurezza*". La norma, infatti, impone che siano preventivamente stabilite le responsabilità e le procedure di gestione per assicurare una risposta rapida ed efficace agli incidenti relativi alla sicurezza delle informazioni.

[159] Cfr. M. PEREGO, *Uscita la nuova ISO 27001:2022 con gli standard su sicurezza delle informazioni, cybersecurity e privacy*, in *Federprivacy*, 2022, in Rete: *https://www.federprivacy.org/informazione/primo-piano/uscita-la-nuova-iso-27001-2022-con-gli-standard-su-sicurezza-delle-informazioni-cybersecurity-e-privacy*; M. PEREGO, *I nuovi controlli della Norma ISO 27001:2022 che impattano sui dati personali*, in *Federprivacy*, 2022, in Rete: *https://www.federprivacy.org/informazione/primo-piano/i-nuovi-controlli-della-norma-iso-27001-2022-che-impattano-sui-dati-personali*.

[160] Cfr. FEDERPRIVACY, *Cosa è la ISO/IEC 27701?*, 2019, in Rete: *https://www.federprivacy.org/informazione/sapresti-rispondere/cosa-e-la-iso-iec-27701*; M. PEREGO, *La ISO/IEC 27701:2019: la lettura della norma sulla gestione della privacy attraverso le ricorrenze*, in *Federprivacy*, 2022, in Rete: *https://www.federprivacy.org/informazione/primo-piano/la-iso-iec-27701-2019-la-lettura-della-norma-sulla-gestione-della-privacy-attraverso-le-ricorrenze*.

rivestito dai titolari e responsabili del trattamento e prevedendo controlli di sicurezza che possono considerarsi come misure di *accountability*[161].

Tuttavia, ciò non basta a considerare le certificazioni della serie ISO/IEC 27000 valevoli ai sensi del GDPR (e in particolare dell'art. 42 GDPR), in quanto ambedue hanno scopi differenti[162].

In primo luogo, infatti, vi è da evidenziare che l'obiettivo della ISO/IEC 27000 è garantire la sicurezza delle informazioni aziendali e non tanto dei dati personali degli interessati[163], i quali non vengono considerati solo come implicito sottogruppo della categoria Informazioni documentate, ovvero informazioni che devono essere controllate e mantenute da un'organizzazione[164]. Essendo, però, troppo sbilanciate sulla sicurezza informativa, e non sufficienti a garantire una valutazione anche dei processi di sicurezza dei dati personali, queste certificazioni sono inadeguate a tutelare i diritti e le libertà degli interessati e, quindi fuori scopo rispetto all'art. 42 GDPR[165].

In secondo luogo, problematico risulta anche l'impostazione strutturale da cui le certificazioni ISO/IEC 27000 discendono. Tali schemi, in quanto ricadenti nell'insieme delle ISO/IEC 17021, prevedono che la certificazione venga fatta come 'sistema di gestione', ossia su un contesto più generale ed ampio, occupandosi di verificare la sola presenza di un dato requisito che rientri in un sistema (di qualità, di sicurezza, …). Il GDPR, all'opposto, prevede che la certificazione venga fatta su un trattamento di dati personali, in quanto afferente ad un prodotto, processo o servizio, occupandosi di avvalorare la corrispondenza tra le caratteristiche del trattamento (cioè il requisito che dev'essere implementato) e la norma terza. Pertanto, il fatto che gli standard ISO/IEC 27000 ricadano in un 'contenitore', il ISO/IEC 17021, diverso da quello richiesto dal Regolamento, ossia il ISO/IEC 17065, determina la non validità delle stesse ai fini del GDPR[166].

---

[161] Ad esempio, per certi aspetti, è stato inserito nella ISO/IEC 27001 anche il principio della *privacy by design*, prevedendo, al controllo A.14.2.1, che: "*la sicurezza delle informazioni sia parte integrante di tutto il ciclo di vita dei sistemi informativi*".

[162] Al più la ISO/IEC 27001, e i suoi controlli, possono essere considerati parzialmente rispondenti alle esigenze di sicurezza richieste dal GDPR. Cfr. M.A. SALVI, *Certificazioni privacy e certificazioni GDPR: quali sono e perché non sono la stessa cosa*, in *Cybersecurity360*, 2021, in Rete: *https://www.cybersecurity360.it/legal/privacy-dati-personali/certificazioni-privacy-e-certificazioni-gdpr-quali-sono-e-perche-non-sono-la-stessa-cosa/.*

[163] Questa differenza è anzitutto apprezzabile sul piano definitorio. Le informazioni, come da standard ISO/IEC27001 sono "*l'insieme di dati che hanno valore per un individuo o un'organizzazione*", mentre i dati personali sono, ai sensi dell'art. 4 GDPR: "*qualsiasi informazione riguardante una persona fisica identificata o identificabile*". Nella categoria delle informazioni, pertanto, si trova qualsiasi tipo di dato, riferibile a qualsiasi contesto. I dati personali, invece, appartengono alla persona fisica a cui si riferiscono. Cfr. R. CASTROREALE, C. PONTI, *Il sistema integrato per la sicurezza delle informazioni ed il GDPR: guida operativa all'efficace integrazione dei due mondi anche con l'ausilio della ISO/IEC 27701*, *op.cit.*, 16.

[164] Sulla scorta di questa critica, come precedentemente indicato, sono state rilasciate le certificazioni ISO/IEC 27001:2022 e ISO/IEC 27701:2019.

[165] Come sottolineato dal WP29, la certificazione della protezione dei dati deve essere chiaramente incentrata sulla protezione dei dati e non deve essere confusa con la sicurezza IT, con la conseguenza che le norme ISO esistenti non coprono pienamente la protezione dei dati personali. Cfr. WP29, *Fablab "GDPR/from concepts to operational toolbox, DIY"- Results of the discussion,* 2017.

[166] Tale circostanza è stata ribadita da Accredia anche in relazione alla ISO/IEC 27701:2019: "*anche se molti argomenti trattati dalla Norma hanno riscontro in specifici requisiti di legge nazionali, sia in Italia,*

Tuttavia, come precedentemente ribadito, la presenza di un sistema di gestione per la sicurezza delle informazioni derivante dalla conformità ad una certificazione ISO, può essere considerato come prova di esistenza di una misura (organizzativa) di sicurezza adeguata al Regolamento[167].

6.2 Normativa UNI 11697:2017: formazione e certificazione dei DPO

La norma UNI 11697:2017 "Attività professionali non regolamentate - Profili professionali relativi al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza" e la relativa prassi di riferimento UNI/PdR 66:2019 definiscono i requisiti di competenza e le regole per la valutazione della conformità di alcune figure professionali che operano nel settore del trattamento e della protezione dei dati personali, quali DPO, *Privacy auditor* e *Privacy specialist*[168]. In quanto orientata alla certificazione di persone, tuttavia, tale certificazione non rientra tra quelle disciplinate dall'art. 42 GDPR per certificare la conformità dei trattamenti. La norma UNI 11697:2017, al più, può rappresentare uno strumento valido per la dimostrazione del possesso delle conoscenze, abilità e competenze professionali necessarie per operare nel contesto dei trattamenti dei dati personali[169].

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 ISO 17065", cfr. ACCREDIA, *Circolare tecnica DC N° 10/2019 – Disposizioni in merito all'accreditamento norma ISO/IEC 27701*, 2019, in Rete: *https://www.accredia.it/documento/circolare-tecnica-dc-n-10-2019-disposizioni-in-merito-allaccreditamento-norma-iso-iec-27701/*. Oltre a ciò, anche lo studio *Data Protection Certification Mechanisms,* commissionato dalla Commissione europea all'Università di Tilburg ha considerato la ISO/IEC 27001 "*out of scope rispetto all'art. 42*", cfr. Commissione europea, *Data Protection Certification Mechanisms Study on Articles 42 and 43 of the Regulation (EU) 2016/679*, 2019, in Rete: *https://commission.europa.eu/system/files/2019-04/data_protection_certification_mechanisms_study_publish_0.pdf*.

[167] Questa interpretazione è stata avvalorata anche dal Garante. Sul punto v. GPDP*, Provvedimento generale del Garante prescrittivo in tema di biometria, Registro dei provvedimenti n. 513 del 12 novembre 2014*; GPDP*, Parere del Garante sull'affidamento della gestione del sistema informativo della fiscalità alla Sogei S.p.a., Registro dei provvedimenti n. 68 del 13 febbraio 2014.*

[168] Lo schema, tuttavia, rimane di puramente volontario, perciò non costituisce titolo necessario per svolgere tali ruoli. Cfr. GPDP, *Faq sul Responsabile della Protezione dei Dati (RPD), https://www.garanteprivacy.it/faq-sul-responsabile-della-protezione-dei-dati-rpd-in-ambito-privato;* FEDERPRIVACY*, Certificazione DPO: i chiarimenti del Garante sulla Norma UNI, 2018, https://www.federprivacy.org/attivita/certificazione-dpo-i-chiarimenti-del-garante-sulla-norma-uni.*

[169] È opportuno segnalare la sua importanza soprattutto per il personale responsabile delle valutazioni e decisioni prese da un Organismo di Certificazione accreditato, il quale deve rispettare una serie di requisiti con riguardo alla norma ISO/IEC 17065:2012 e ai Requisiti di accreditamento aggiuntivi dal Garante per la protezione dei dati personali.

CAPITOLO II - LE CERTIFICAZIONI PER LA PROTEZIONE DEI DATI PERSONALI AI SENSI DEL REGOLAMENTO UE 2016/679

1 Gli strumenti di autoregolazione volontaria nel GDPR: una breve panoramica sui codici di condotta

Da diverso tempo il Legislatore europeo ha intrapreso una politica normativa volta ad incentivare l'autoregolamentazione da parte dei privati. Il settore della protezione dei dati personali costituisce un esempio lampante di questo metodo, il quale è stato riproposto anche in recenti interventi legislativi, fra cui il *Digital Service Act*[1] e la Direttiva AVMS[2]. Inoltre, vi è da sottolineare che l'utilizzo dell'autoregolamentazione nel settore *data protection* non costituisce affatto una novità del Regolamento. Infatti, a partire dalla Direttiva Madre, la Commissione ha introdotto, anche se con una disciplina alquanto sommaria, i codici di condotta nell'ambito privacy, incoraggiando l'adozione delle prime forme di regolamentazione trasversale della disciplina sulla protezione dei dati personali da parte delle associazioni professionali e imprenditoriali[3]. Questi elementi, successivamente, sono stati trasportati in una nuova politica di *governance* europea fondata su una maggiore partecipazione dei privati nelle istituzioni dell'Unione e nei processi regolativi e amministrativi, al fine di aumentare la fiducia dei cittadini nelle politiche europee[4].

Il GDPR ha, quindi, raccolto i risultati raggiunti dalla prosecuzione di questa politica, nonché soprattutto dai vent'anni di vigenza della Direttiva 95/46/CE e li ha trasposti nelle previsioni relative ai codici di condotta (art. 40-41) e certificazioni, sigilli e marchi (art. 42-43), creando un compiuto sistema di autoregolamentazione, da parte dei privati, degli adempimenti in materia *data protection*.

Nel capitolo precedente si è accennato al fatto che le certificazioni costituiscono una modalità di autoregolamentazione privata attraverso la fornitura di *standard* univoci tra determinati soggetti e lo sviluppo della conformità intorno ad essi (con conseguente verifica e attestazione di un simbolo). L'assetto appena evidenziato,

---

[1] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/ce (regolamento sui servizi digitali – *digital service act*).

[2] Direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio del 14 novembre 2018 recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), in considerazione dell'evoluzione delle realtà del mercato.

[3] In particolare, l'elaborazione ed adesione a codici di condotta nazionali o di portata europea (in quanto promossi dalla Commissione e approvati dal WP29), come previsto dal considerando n. 61: "*gli Stati membri e la Commissione, nei rispettivi settori di competenza, devono incoraggiare gli ambienti professionali interessati a elaborare codici di condotta destinati a favorire, secondo le caratteristiche specifiche dei trattamenti effettuati in taluni settori, l'attuazione della presente direttiva nel rispetto delle disposizioni nazionali di applicazione della stessa*" e dall'art. 27: "*1. Gli Stati membri e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione della presente direttiva, adottate dagli Stati membri*" Direttiva 95/46/CE.

[4] Cfr. Commissione europea, *COM/2001/428, "La governance europea – Un libro bianco*", 2001.

tuttavia, costituisce solamente una particolare forma e modalità di partecipazione dei privati ai processi regolativi, in un contesto che ammette forme di regolamentazione privata sulla base di diversi principi.

Un criterio generale, ma preminente fra tutti i diversi parametri, attiene alla natura dei soggetti partecipanti alla regolamentazione e alla qualità della stessa; proprio su questo punto, difatti, si può distinguere tra 'autoregolamentazione' e 'co-regolamentazione'. Dell'autoregolamentazione si è già detto che consiste nella "*possibilità lasciata agli operatori economici, alle parti sociali, alle organizzazioni non governative o alle associazioni di adottare tra di loro e per sé stessi orientamenti comuni, non presupponendo una presa di posizione da parte delle istituzioni*"[5]. Sulla base dello schema sopradescritto, vi è da riconoscere che la natura della regolamentazione prodotta sarebbe sicuramente di base negoziale, in cui i vari attori della società civile si riunirebbero per creare delle norme in uno spazio dell'ordinamento giuridico vuoto, o meglio, in un ambito in cui è lo stesso ordinamento a riconoscere la creazione di norme al di fuori delle fonti istituzionali[6]

Tuttavia, questo strumento non è stato giudicato congruo ed equilibrato rispetto ai diversi interessi in gioco presenti in determinati settori legislativi, quali la disciplina della protezione dei dati personali, tali per cui solo la figura del Legislatore pare l'unica legittimata a bilanciarli [7]. Pertanto, risulta necessaria una forma di controllo dell'autoregolamentazione che non si risolva in una mera eterodirezione, e ciò lo si ha proprio con la co-regolamentazione.

Sempre il Progetto Interistituzionale "Legiferare Meglio" definisce la co-regolazione come: "*il meccanismo mediante il quale un atto legislativo comunitario conferisce la realizzazione degli obiettivi dell'autorità legislativa ai soggetti interessati riconosciuti in un determinato settore (operatori economici, parti sociali, ONG, associazioni di categoria)"*[8]. La co-regolazione, quindi, si comporrebbe di due livelli: il primo è dato da un atto legislativo, il quale esprime i principi e i criteri di base su cui dovrà svilupparsi la regolamentazione privata; il secondo è proprio l'intervento dei privati, i quali possono concludere accordi per stabilire le modalità di esercizio di una data attività, sulla base dei criteri prefissati dalla norma di legge [9]. Quanto detto, rappresenterebbe proprio un approccio regolativo "*top-down"* il quale, attraverso il

[5] Cfr. Parlamento Europeo, Consiglio Europeo, Commissione europea, *Progetto Interistituzionale - «Legiferare meglio»*, *op. cit.*, punto 22. Sul punto vedasi quanto riportato nel capitolo 1.5.

[6] Cfr. N. LIPARI, *La formazione negoziale del diritto*, in Riv. dir. civ., 1987, I, p. 315. L'autore, infatti, riconosce come la formazione negoziale del diritto sia "*un connotato essenziale della stessa positività dell'ordinamento giuridico*", in quanto è lo stresso ordinamento che consentirebbe la creazione di regole che non promanano dall'alto, cioè dalle istituzioni pubbliche, ma provenienti dal basso, cioè dagli attori privati. Sul punto, inoltre, v. T. GALLETTO, *71. Codici di condotta*, *Digesto Civile*, Torino, 2011, p. 163.

[7] Cfr. G. ALPA, *Autodisciplina e codici di condotta*, in *Sociologia del diritto*, fasc. 2, 1995, 128 ss.

[8] Cfr. PARLAMENTO EUROPEO, CONSIGLIO EUROPEO, COMMISSIONE EUROPEA, *Progetto Interistituzionale - «Legiferare meglio», op.cit.*, punto 18.

[9] Cfr. *ivi,* al punto 20, precisa che "*nel contesto definito dall'atto legislativo di base, i soggetti interessati possono concludere accordi autonomi per stabilire le modalità" e punto 19 "l'atto legislativo deve rispettare il principio di proporzionalità del Trattato Ce. Gli accordi tra le parti sociali devono rispettare le disposizioni previste agli artt. 138 e 139 del Trattato CE".*

coordinamento fra i regolatori pubblici e le parti private interessate, andrebbe a produrre regole specifiche e dettagliate ovvero la definizione di standard uniformi[10].

Si farebbe dunque riferimento ad una sorta di regolamentazione pubblicistica dell'autoregolazione privata, con la conseguenza che varierebbero, rispetto a quest'ultimo modello, anche i ruoli di determinazione delle regole e di vigilanza attribuiti alle parti in gioco: ad esempio, la funzione di regolazione ad un privato, e quella di supervisione ad un regolatore pubblico, oppure forme di partenariato pubblico e privato in entrambe, o altre modalità ancora[11].

Gli aspetti positivi di questo modello sono dati dalla partecipazione dei privati nei processi regolativi e nel controllo della loro attuazione. Questi ultimi, essendo i soggetti maggiormente coinvolti dalle stesse regole, sono coloro che permettono di garantire maggiore specificità alle azioni, astratte e generali, decise a livello legislativo. La conoscenza e l'esperienza pratica degli operatori privati, determinerebbe una maggiore padronanza delle politiche oggetto di regolazione lasciando comunque spazio alle autorità pubbliche di intervenire per rimuovere eventuali assetti giudicati inadeguati con le garanzie poste a principio dell'ordinamento e della co-regolazione[12].

Il presente schema è anche quello adottato dalla disciplina presente negli artt. 40 e successivi del GDPR. Infatti, accanto allo sviluppo dell'autoregolamentazione privata in tema di adempimenti connessi alla normativa sulla protezione dei dati personali, rimane sempre affiancata l'autorità di controllo nazionale quale soggetto posto a garante della disciplina *privacy* e della tutela dei diritti e libertà dei cittadini europei.

L'Importanza e l'evoluzione di tali strumenti nella disciplina del Regolamento può essere ricondotta a quattro principali elementi.

In primo luogo, la necessaria specializzazione degli adempimenti *privacy* connessi ai vari settori dell'economia e della tecnologia rende necessario avere un disciplinare di riferimento più approfondito e pratico della normativa europea, su cui titolari e responsabili del trattamento possano appoggiarsi al fine di costruire un sistema di compliance flessibile, efficiente e altamente specializzato, in modo da adattarsi al segmento specifico di attività delle imprese[13].

In secondo luogo, con lo sviluppo del *Digital Single Market* e l'obiettivo della libera circolazione dei dati all'interno dell'Unione, il GDPR mira ad incrementare la fiducia degli utenti nell'utilizzo dei prodotti e servizi digitali, rassicurandoli circa il trattamento dei

[10] Cfr. L. SENDEN, *Soft Law, Self-Regulation and Co-Regulation in European Law: Where Do They Meet?*, in *Electronic Journal of Comparative Law*, vol. 9.1, 2006, p. 11.

[11] Cfr. A.R. POPOLI, *Codici di condotta e certificazioni*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, 367-373. Sul punto, quindi, è importante ribadire che la co-regolazione non comporta, a differenza dell'autoregolazione, una deregolazione, in quanto le autorità pubbliche rimangono coinvolte in tutte le fasi del processo normativo: dalla definizione degli standard normativi di principio, alla valutazione di adeguatezza della regolazione nonché in sede di *enforcement*.

[12] Cfr. COMMISSIONE EUROPEA, *COM/2001/428, "La governance europea – Un libro bianco*", 2001.

[13] Proprio in relazione a ciò, il considerando n. 98 GDPR raffigura come "*i codici di condotta potrebbero calibrare gli obblighi dei titolari del trattamento*", specificando gli adempimenti del Regolamento tenendo sempre conto "*del potenziale rischio per i diritti e le libertà delle persone fisiche*". Il contenuto dei codici di condotta, poi, dev'essere relazionato altresì alle "*esigenze specifiche delle micro, piccole e medie imprese*" garantendo il carattere di flessibilità che il GDPR assegna agli obblighi di *accountability.*

loro dati personali da parte degli operatori economici[14]. A fronte di ciò, l'uso di certificazioni e sigilli, per le capacità comunicative e di marketing precedentemente segnalate, risulterebbe funzionale a garantire questa fiducia[15].

In terzo luogo, la nuova disciplina appare incentrata essenzialmente sui processi, attività, misure tecniche e organizzative rivolte al titolare del trattamento e, come evidenziato nel precedente capitolo, la chiave di volta di questo sistema è il principio di *accountability.* I modelli di co-regolazione previsti nel Regolamento, sotto questo profilo, costituiscono uno strumento di agevolazione nella dimostrazione della *compliance* del titolare o responsabile alla normativa europea.

A fronte di ciò, risulta emblematico lo stretto collegamento fra il principio di *accountability* e i sistemi di co-regolamentazione come immaginati dal Legislatore europeo. Codici di condotta e certificazioni, infatti, risulterebbero degli strumenti flessibili e adattabili a garantire l'effettiva applicazione delle regole e dei principi del GDPR, fra cui anche il rafforzamento delle misure rivolte a dimostrare la propria *compliance* a quest'ultimo[16]. A ciò bisogna aggiungere che il passaggio da un sistema gerarchico e centralizzato, come previsto dalla Direttiva Madre e dal Codice Privacy, ad un sistema decentralizzato che ruota intorno alla figura del titolare del trattamento e del suo essere *accountable*, ha reso necessario puntare su meccanismi e strumenti ulteriori che consentano di specificare gli adempimenti previsti per la tutela dei diritti e libertà degli interessati.

Oltre ai pareri dell'EDPB e ai provvedimenti del GPDP, i codici di condotta e le certificazioni costituiscono i principali "*accountability tools"*[17] previsti dal Regolamento. Di fatti, questi, venendo genericamente enunciati dal considerando n. 100, quali strumenti rivolti a migliorare la trasparenza e il rispetto del GDPR, rilevano secondo gli artt. 5, par. 2 e 24, par. 3 quali mezzi per dimostrare il rispetto degli obblighi tecnici e organizzativi del titolare del trattamento, nonché per efficacemente attuare i principi della privacy *by design* e privacy *by default, ex* art. 25, par. 3. Costituiscono, ai sensi dell'art. 28, par. 5 e considerando n. 81, un elemento volto a valorizzare l'attestazione delle capacità del responsabile del trattamento, al fine che questi possa dimostrare le garanzie necessarie per mettere in atto misure tecniche e organizzative adeguate a

[14] Cfr. considerando n. 7 GDPR: "*Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno*". Inoltre, v. COMMISSIONE EUROPEA, *COM/2015/192, 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*, 2015, in Rete: *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52015DC0192&from=DE*.

[15] Cfr. F. PIZZETTI, *La protezione dei dati personali e la sfida dell'intelligenza artificiale*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, p. 170.

[16] Cfr. COMMISSIONE EUROPEA, *COM/2010/609, Comunicazione della commissione europea del 4 novembre 2010, Un approccio globale alla protezione dei dati personali dell'Unione europea*, 2010, p.14, in Rete: *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52010DC0609&from=SK*.

[17] Cfr. EDPB, *Accountability Tools*, in Rete: *https://edpb.europa.eu/accountability-tools_en*; D. POLETTI, M.C. CAUSARANO, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione, op.cit.,* 396.

soddisfare i requisiti del Regolamento[18]. Ulteriormente a ciò, l'art. 28, par. 6 nomina le certificazioni quali basi su cui poter sviluppare le clausole relative al contratto tra titolare e responsabile del trattamento. Inoltre, determinano, ai sensi del considerando n. 77, un insieme di regole da rispettare in sede di valutazione d'impatto di cui all'art. 35, par. 8, al fine di individuare efficacemente i rischi derivanti dal trattamento e a mettere in atto le misure più opportune per attenuarne la portata, nonché quali strumenti per dimostrare la predisposizione di misure tecniche ed organizzative adeguate a garantire un livello di sicurezza adeguato del trattamento *ex* art. 32, par. 3. Infine, l'art. 83, co. 2, lett. j) considera l'adozione di uno dei suddetti strumenti, da parte di titolari e responsabili del trattamento, come uno dei parametri di quantificazione della sanzione amministrativa[19].

Tutti questi elementi dovrebbero, quindi, esaltare la cooperazione fra le istituzioni pubbliche e i portatori di interessi privati per creare un sistema preciso, completo e composito al fine di garantire un maggiore livello di effettività dei precetti del Regolamento e della loro applicazione.

Tali considerazioni sono determinanti nel comprendere l'evoluzione dei codici di condotta e dei meccanismi di certificazione, quali mezzi di co-*regulation* nella regolazione europea della *data protection*.

Pur proseguendo, nei successivi paragrafi, con la disamina del sistema delle certificazioni previsto dal GDPR, risulta doveroso, al fine di fornire una visione d'insieme di tutti i mezzi di *accountability*, procedere ad una breve e preliminare analisi della disciplina in tema di codici di condotta, di cui agli artt. 40 e 41 del Regolamento.

I codici di condotta, nell'ambito della protezione dei dati personali, risultano presenti già a partire dalla Direttiva Madre, ove se ne prevedeva, tuttavia, solamente di incoraggiarne lo sviluppo[20]. La *ratio* principale di tale opzione regolativa era quella di definire, insieme ai soggetti interessati[21], misure tecniche e prassi specifiche, in relazione ad ambiti operativi differenziati, al fine di sostanziare i principi della protezione dei dati personali. Inoltre, la flessibilità di tali strumenti ne consentiva, ove necessario, la modifica, l'integrazione o l'aggiornamento in modo più agevole rispetto agli ordinari procedimenti legislativi. Ciò determinava il vantaggio di avere un constante e adeguato

[18] Le medesime valutazioni, poi, potranno essere utilizzate dal responsabile del trattamento in sede di eventuale nomina di un *sub*-responsabile, cioè quei soggetti a cui il responsabile del trattamento si rivolge per affidargli l'esecuzione di specifiche attività del trattamento di dati personali per conto del titolare del trattamento.

[19] Cfr. D. POLETTI, M.C. CAUSARANO, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione, op.cit.,* 379.

[20] Cfr. considerando n. 61 GDPR: "*gli Stati membri e la Commissione, nei rispettivi settori di competenza, devono incoraggiare gli ambienti professionali interessati a elaborare codici di condotta destinati a favorire, secondo le caratteristiche specifiche dei trattamenti effettuati in taluni settori, l'attuazione della presente direttiva nel rispetto delle disposizioni nazionali di applicazione della stessa*" e art. 27: "*1. Gli Stati membri e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione della presente direttiva, adottate dagli Stati membri*".

[21] La finalità di coinvolgere i privati nell'elaborazione di tali regole è data dal fatto che, particolarmente nei codici di condotta, la partecipazione dei soggetti interessati al processo elaborativo delle regole di condotta che devono loro applicarsi può accrescerne il grado di conoscenza dell'ambiente normativo in cui operano e, di conseguenza, promuovere la loro responsabilizzazione.

sistema di regole la cui vigenza si sarebbe esplicata in contesti applicativi esposti agli effetti di rapidi mutamenti tecnologici ed economici[22].

In questo modo, parallelamente alle leggi di attuazione degli Stati membri, si sarebbero potuti affiancare strumenti regolativi sorti dalla collaborazione tra soggetti pubblici ed attori privati, la cui adozione, in quanto destinata ad integrare settorialmente la normativa generale, sarebbe valsa ad organizzare in un sistema reticolare le fonti giuridiche rilevanti per la tutela dei dati personali[23].

Consolidando alcune caratteristiche già presenti nella vigenza della Direttiva Madre e della normativa nazionale di attuazione (primo fra tutti il Codice Privacy), l'impianto normativo del Regolamento sui codici di condotta si basa su una serie di caratteristiche fondamentali.

Due fra queste riguardano la portata applicativa dei codici di condotta: in primo luogo, rispetto ad altri strumenti autoregolamentativi, quali gli autodisciplinari sperimentati nel mondo imprenditoriale, le regole contenute nei codici, in ragione della loro finalità integrativa, sono generalmente applicabili ad un dato settore, senza tener conto dell'adesione ad eventuali ordini professionali [24]. Questo effetto è dato principalmente dall'intervento dell'autorità pubblica, finalizzato ad assicurare che le regole e le responsabilità previste dai codici convergevano con gli obiettivi della precedente disciplina[25].

In secondo luogo, lo sviluppo dei modelli deontologici da parte degli operatori economici ha diretto i codici di condotta ad avere una fisionomia settoriale o multisettoriale e contenuti circoscritti ad una o più, ma comunque collegate, attività professionali[26]. Tale sviluppo ha determinato la necessità per cui, l'ambito applicativo delle prescrizioni contenute nei codici non doveva determinarsi sulle caratteristiche soggettive di un dato individuo/ente, ma oggettive, ossia sullo svolgimento di una determinata attività.

---

[22] Cfr. R. D'ORAZIO, *Articolo 40 – Codici di condotta*, in E. BELISARIO, G.M. RICCIO, G. SCOZZA (a cura di), *GDPR e Normativa Privacy*, Milano, 2020, 445-467.

[23] In relazione a ciò, i codici di condotta sono stati qualificati dalla dottrina come fonte secondaria atipica, in virtù della sua base legislativa e della portata applicativa delle sue previsioni ampia. Sul punto v. A. SIMONCINI, *I codici deontologici di protezione dei dati personali nel sistema delle fonti. L'emersione di un nuovo paradigma normativo?*, in *Osservatorio sulle fonti*, 1999, 282, in Rete: *https://www.osservatoriosullefonti.it/archivi/archivio-volumi-osservatorio/osservatorio-1999/60-11-andrea-simoncini/file*.

[24] Cfr. T. ANNECCA, *Codici deontologici e il GDPR*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Milano, 2019, 628. L'autrice, in particolare, sottolinea specificatamente che i codici di condotta, a differenza dei 'codici di deontologia', sarebbero diretti a disciplinare settori nei quali manchi un ordine professionale di rilievo pubblicistico, e siano invece unicamente presenti associazioni libere di categoria o di settore.

[25] Coerentemente con le previsioni sui sistemi di certificazione, infatti, viene ribadita la centralità delle procedure di co-decisione tra l'Autorità nazionale di controllo e le parti interessate alla definizione delle regole dei codici di condotta. Come stato individuato da autorevole dottrina, l'autorità nazionale di controllo rappresenterebbe la 'valvola' attraverso cui le regole deontologiche si conformano all'ordinamento generale e sono da questo assimilate, per divenire fonti giuridiche di valenza erga omnes. Cfr. R. D'ORAZIO, *Articolo 40 – Codici di condotta*, *op.cit.*, 445-467.

[26] Con la conseguenza che potrebbero ben essere adottati anche più codici in relazione a singole tipologie di trattamenti posti in essere in una determinata professione o nell'ambito di uno stesso comparto operativo.

In terzo luogo, per quanto concerne lo scopo, il Regolamento attribuisce ai codici la finalità di "*contribuire alla corretta applicazione del […] Regolamento, in funzione della specificità dei vari settori di trattamento e delle esigenze delle micro, piccole e medie imprese*". In questo modo, i codici di condotta dovrebbero individuare le *best practice* sul trattamento di dati personali in determinati settori, sulla base dell'esperienza delle organizzazioni rappresentative, come modalità per assicurare la conformità dei trattamenti ai principi del Regolamento e dell'eventuale normativa di settore.

Il summenzionato scopo è poi coerente con la valenza probatoria assegnata dal GDPR all'adesione ad un codice di condotta. Infatti, come previsto nell'art. 40, la circostanza per cui titolare o responsabile abbiano aderito ad un codice di condotta comporta, per questi ultimi, un'attenuazione dell'onere probatorio relativo alla dimostrazione del rispetto degli adempimenti previsti dal regolamento, primi fra tutti il rispetto dei principi di *accountability* e *privacy by design*, similmente a quanto accade per il conseguimento di una certificazione[27].

Rispetto a quanto previamente detto, la normativa nazionale assegna ai codici di condotta un ulteriore valenza rispetto a quella del Regolamento. L'art. 2-*quater* del Codice Privacy, infatti, conferisce al rispetto delle regole contenute nei codici di condotta approvati nell'ordinamento nazionale italiano, condizione essenziale per la liceità e la correttezza per i trattamenti dei dati personali relativi ai codici adottati. Come sottolineato da parte della dottrina, con l'attribuzione di un ulteriore condizione di liceità del trattamento al rispetto delle regole deontologiche, il Legislatore pare abbia voluto forzare l'art. 6 par. 2-3 del Regolamento. Tuttavia, secondo altra parte della dottrina, la scelta italiana di porre sul medesimo piano i codici di condotta approvati agli adempimenti del GDPR, sarebbe da accogliere in quanto, nel nostro ordinamento, i codici di condotta sono rivolti a regolamentare i trattamenti di dati personali di cui il Regolamento, al Capo IX, ha affidato la disciplina ai singoli Stati membri[28]. Con questa scelta di campo, il Legislatore italiano garantirebbe che la disciplina di settore sia affidata a meccanismi autoregolamentativi, assicurandosi comunque che quest'ultima rientri nel perimetro di immediata vincolatività derivante dalla legge, per chiunque esegua i trattamenti su cui insistono i codici.[29]

---

[27] Nel Regolamento, sono molti i casi in cui lo stesso prevede esplicitamente che i codici di condotta valgono come dimostrazione del principio di *accountability*. In particolare: in tema di: sussistenza delle garanzie sufficienti alla designazione del responsabile, in caso di adesione di quest'ultimo ad un codice di condotta approvato (art. 28, par. 5 GDPR); nell'adozione di misure tecniche adeguate a garantire la sicurezza del trattamento (art. 32, par. 3 GDPR); nella previsione di garanzie adeguate per il trasferimento transfrontaliero di dati (art. 46, par. 2, lett. e) GDPR); per la valutazione d'impatto sulla protezione dei dati personali (art. 35, par. 8 GDPR). Infine, la sottoscrizione rappresenta un motivo di attenuazione (od esonero) della responsabilità dell'aderente per le violazioni compiute, figurando fra le attenuanti di cui l'autorità deve tener conto (art. 83, par. 2, lett. j) GDPR).

[28] In particolare, Articolo 85 Trattamento e libertà d'espressione e di informazione; Articolo 86 Trattamento e accesso del pubblico ai documenti ufficiali; Articolo 87 Trattamento del numero di identificazione nazionale; Articolo 88 Trattamento dei dati nell'ambito dei rapporti di lavoro; Articolo 89 Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici; Articolo 90 Obblighi di segretezza; Articolo 91 Norme di protezione dei dati vigenti presso chiese e associazioni religiose.

[29] Cfr. R. D'ORAZIO, *Articolo 40 – Codici di condotta*, *op.cit*., 445-467. Sul punto, l'autore sottolinea, inoltre, che "*Rispetto agli spazi lasciati dal GDPR per gli ulteriori ambiti di trattamento lasciati alla disciplina*

Infine, gli ultimi due aspetti di cui si deve tenere conto riguardano il diverso valore dei codici di condotta all'interno del territorio dell'Unione europea.

La dottrina, infatti, evidenzia come il Regolamento individui tre tipologie di codici di condotta: quello avente carattere meramente nazionale, quello rivolto ad attività di trattamento in diversi Stati membri ed infine i codici di condotta aventi validità generale all'interno dell'Unione [30]. La differenza fra questi attiene al carattere dualistico composto, per un verso, dalle procedure rivolte all'approvazione delle regole di condotta e, per l'altro, dalla validità sovrannazionale delle stesse. Infatti, se per i codici nazionali, l'autorità competente a pronunciarsi in ordine alla conformità al Regolamento dei codici deontologici, nel caso in cui il progetto di codice, o comunque la modifica o la proroga di uno già esistente, riguardasse attività di trattamento svolta in vari Stati membri, l'autorità nazionale di controllo a cui è stato presentato il progetto, in sede di valutazione di conformità dovrà coinvolgere, quali co-revisori, le altre autorità nazionali di controllo interessate dallo stesso[31] e, inoltre, a conclusione delle verifiche preliminari, dovrà sottoporre il progetto all'EDPB il quale si pronuncerà con parere in merito all'approvazione finale[32]. Trattandosi, di fatto, di un codice che dovrà operare a livello sovrannazionale, il meccanismo di cooperazione con le altre autorità di controllo e il controllo del Comitato sono assolutamente necessari per assicurare coerenza e omogeneità nell'applicazione del Regolamento[33]. La terza tipologia di codice di condotta si ha allorché la Commissione decida, mediante atti di esecuzione e sulla base del parere espresso dal Comitato, che il codice di condotta sottoposto abbia validità generale all'interno dell'Unione.

Infine, i codici di condotta possono avere anche una portata extra-europea. L'art. 40, par. 3, infatti, ammette anche che l'adesione ai codici di condotta sia consentita anche ai titolari o responsabili del trattamento che non siano soggetti al Regolamento ai sensi dell'art. 3, al fine di fornire le "adeguate garanzie" necessarie per il trasferimento dei dati personali verso paesi terzi. In questo modo, si fornisce ai codici di condotta un valore maggiormente pregnante rispetto a quello che avrebbe per i soggetti assoggettati al GDPR, come base per la conformità con i principi europei sulla protezione dei dati[34].

---

nazionale, i codici di condotta, possono costituire per la vocazione attuativa ed integrativa che le connota, la sede delle "norme più specifiche" consentite dal GDPR al legislatore nazionale in date materie, nonché l'alveo di raccolta dell'acquis, ove compatibile, formato dai provvedimenti dell'autorità e dalla sua giurisprudenza".

[30] Cfr. A.R. POPOLI, *Codici di condotta e certificazioni*, *op.cit.*, 397; L. BOLOGNINI, *Art. 20 – Codici di deontologia e di buona condotta vigenti alla data di entrata in vigore del presente decreto*, in L. BOLOGNINI, E. PELINO (diretto da), Codice *della disciplina privacy*, Milano, 2019, 287.

[31] Cfr. EDPB, *Linee-guida 01/2019 sui codici di condotta e sugli organismi di monitoraggio a norma del regolamento (UE) 2016/679*, 2019, 20-21, in Rete: *https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-0_it*.

[32] Per i codici sovrannazionali sarà quindi il Comitato ad esprimere un parere sulla conformità del progetto del codice di condotta al Regolamento. Infine, l'art. 40, par 7, prevede che, qualora il parere del Comitato abbia esito positivo, lo stesso provvede, altresì, a trasmettere il proprio parere alla Commissione.

[33] Proprio il citato meccanismo costituisce attuazione del meccanismo di coerenza di cui all'art. 63 GDPR: "*Al fine di contribuire all'applicazione coerente del presente regolamento in tutta l'Unione, le autorità di controllo cooperano tra loro e, se del caso, con la Commissione mediante il meccanismo di coerenza stabilito nella presente sezione*"

[34] Per approfondire sugli ulteriori requisiti per i codici di condotta per il trasferimento transfrontaliero di dati verso paesi terzi v. A.R. POPOLI, *Codici di condotta e certificazioni*, *op.cit.*, 394-404; L. BOLOGNINI, *Codici*

Ne risulterebbe un ampliamento dell'approccio europeo nei confronti dei paesi terzi, anche in considerazione della natura sovrannazionale e aterritoriale della privacy nel mondo odierno[35].

In conclusione, nell'impianto disegnato dal Legislatore europeo, i codici di condotta rappresentano un importante meccanismo rivolto ad assicurare non solo la conformità al Regolamento, ma anche l'effettiva attuazione dello stesso mediante la definizione di regole comuni tra gli operatori coinvolti in trattamenti. Alla medesima esigenza, come si avrà modo di spiegare nei successivi capitoli, rispondono anche i meccanismi di certificazione, quali strumenti co-regolativi rivolti a specificare mediante regole tecniche gli obblighi normativi, contribuendo alla corretta applicazione del GDPR, e a dimostrare la conformità del trattamento nei confronti delle autorità di controllo.

2 Considerazioni preliminari sulle certificazioni per la protezione dei dati personali: definizioni, scopo e soggetti coinvolti

Meccanismi di certificazione, sigilli e marchi per la protezione dei dati personali rappresentano, per i titolari e responsabili del trattamento, l'altro strumento utile a dimostrare la propria conformità al GDPR. Insieme ai codici di condotta, questi strumenti possono agevolmente ridurre la complessità degli adempimenti relativi ai trattamenti di dati personali, determinando una maggiore certezza nella definizione degli oneri legali e costituendo, altresì, una modalità efficacie per infondere, all'interno del mercato unico digitale, i valori di una *governance* effettiva per la tutela dei dati personali[36].

L'inserimento dei meccanismi di certificazione all'interno del GDPR rappresenta una novità rispetto ai codici di condotta, la cui adozione era già stata 'incoraggiata' con la Direttiva 95/46/CE [37]. Nonostante ciò, è stato proprio durante la vigenza di quest'ultima che si è avvertita la necessità di adottare programmi o sigilli di certificazione, quale effetto del principio di *accountability.* Già il WP29, nel Parere 3/2010[38] aveva sottolineato come la predisposizione di sistemi di certificazione avrebbe potuto contribuire "*a dimostrare che un titolare del trattamento ha rispettato la disposizione e che, quindi, ha definito e attuato misure appropriate che sono state periodicamente sottoposte a revisione*"[39], potendo essere usate anche come strumento

di condotta, in L. BOLOGNINI, C. BISTOLFI, E. PELINO (a cura di), *Il Regolamento Privacy europeo*, Milano, 2019, 425-426.

[35] Per approfondire v. G. PASCUZZI, *Il diritto dell'era digitale,* Bologna, 2020, parte XXI – Deterritorializzazione.

[36] Cfr. D. POLETTI, M.C. CAUSARANO, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione, op.cit.,* 380.

[37] Cfr. *ivi*, 396. Certificazione in tema di sicurezza delle informazioni e protezione dei dati (anche personali) erano comunque già esistenti precedentemente al GDPR nelle varie realtà nazionali, come si specificherà *infra*. La vera novità, tuttavia, risiede nel fatto che mediante il loro inserimento nel Regolamento, si sia previsto una disciplina armonizzata che consente un'applicazione uniforme e coerente di tali meccanismi a livello europeo.

[38] Cfr. WP29, *Parere 3/2010 sul principio di responsabilità, op.cit.*, 18-19.

[39] Cfr. *ivi*, punto 68. In particolare, un settore in cui si ipotizzava l'utilità delle certificazioni era individuato nel trasferimento transfrontaliero di dati personali, nella dimostrazione, da parte del titolare del trattamento, di aver messo in atto adeguate garanzie. I servizi certificatori si occuperebbero, infatti, di analizzare le assicurazioni fornite dal titolare del trattamento.

per distinguersi all'interno del mercato al fine di acquisire un vantaggio competitivo. Ciononostante, la messa a punto di sistemi di certificazione per la tutela dei dati personali (senza considerare le norme tecniche ISO), precedentemente al GDPR, è stata scarseggiante e limitata esclusivamente ad alcuni Stati membri, anche in ragione della frammentazione della normativa di recepimento in materia di protezione dei dati personali.

Alla luce di questa situazione, è facile capire perché il Legislatore europeo volesse regolamentare esattamente questi strumenti. A fronte dell'impossibilità di dettare delle regole giuridiche comuni che vadano ad uniformare gli obblighi tecnico-operativi di titolari e responsabili del trattamento, si è inteso far uso ad una diversa forma di regolazione e standardizzazione[40]. Infatti, le certificazioni, a differenza delle norme giuridiche, non incontrano i limiti dati dalle varie tradizioni giuridiche che contraddistinguono le singole nazioni europee[41], permettendo di specializzare la regolamentazione tecnica relativa alla *data protection* attraverso la predisposizione di un meccanismo di certificazione completo e, tendenzialmente, comune a tutti gli Stati membri.

Le certificazioni costituiscono, per i titolari e responsabili del trattamento, un mezzo che permette di dimostrare di aver adottato delle misure tecniche ed organizzative efficaci e tali da soddisfare, nella prospettiva *risk-based* che permea il GDPR, il principio di *accountability*. In quest'ottica, le imprese potranno dimostrare di aver adottato le misure più idonee in relazione ai rischi individuati nel trattamento di dati personali. Proprio l'elemento dimostrativo è ciò che differenzia gli strumenti co-regolativi del Regolamento rispetto alla normativa precedente: se in costanza della Direttiva Madre e del Codice Privacy, l'adesione ad un codice di condotta era una condizione di liceità, ora, ai sensi del GDPR, certificazioni e codici rappresentano elementi probatori da poter esibire per dimostrare e rendere manifesto il rispetto degli obblighi del titolare o responsabile del trattamento di fronte al pubblico e, eventualmente, alle autorità di controllo competenti[42].

Proprio la possibilità di aderire volontariamente ad uno schema di certificazione è l'elemento fondante del sistema, in quanto consente di valorizzare le strategie

[40] D'altronde vi è da dire che l'assenza di norme tecniche di dettaglio, all'interno del Regolamento, circa le possibili misure tecniche ed organizzative implementabili non è frutto di una 'svista' del Legislatore europeo, ma di una precisa scelta di non ancorare la regolamentazione a dei canoni che rischiavano un'obsolescenza prematura. A tal proposito, invece, si è optato per promuovere genericamente una serie di attività rivolte ad implementare le misure tecniche ed organizzative richieste dai principi della *privacy by design* e *privacy by default*, aprendo la possibilità agli attori coinvolti nel trattamento di dati personali di adottare ogni misura ritenuta congrua e utile a dimostrare la conformità a terzi, anche mediante codici di condotta e certificazioni.

[41] Cfr. G.M. RICCIO, V. VITI, *Le "Certificazioni privacy" ed il Regolamento UE*, in *MediaLaws*, 2017, in Rete: *https://www.medialaws.eu/le-certificazioni-privacy-ed-il-regolamento-ue/*. In particolare, l'a. sottolinea che "*le certificazioni non incontrano i limiti delle regole giuridiche, dal momento che non risentono delle singole tradizioni nazionali e sono identiche per tutti gli Stati membri.*"

[42] Cfr. S. SILEONI, *I codici di condotta e le funzioni di certificazione*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I Dati Personali Nel Diritto Europeo*, Torino, 2019, 932, ove l'a. evidenzia chiaramente come certificazioni e codici di condotta rientrerebbero "*ai sensi dell'art. 24, comma 3 nel novero di quelle prove che il responsabile o il titolare del trattamento ha l'onere di fornire per attestare di aver attuato tutte le misure organizzative e di sicurezza adeguate alla specifica tipologia di dati*".

intraprese dal titolare o responsabile del trattamento. Questi ultimi, mediante un'attestazione fornita da parte di un ente indipendente, possono dimostrare al mercato la correttezza delle misure tecniche ed organizzative scelte ed implementate per la protezione dei dati personali, nonché la competenza sviluppata mediante l'individuazione delle stesse. L'istituzione di tale certificazione permette, dunque, di affermare apertamente il livello di conformità dell'impresa, evidenziando agli interessati il fatto di aver adottato una metodologia di analisi e attuazione del Regolamento idonea a garantire la protezione dei dati personali.

Come illustrato in queste considerazioni preliminari, la certificazione, ai sensi dell'art. 42, par. 3 è volontaria; l'adesione ad essa non è imposta, ma è basata su una scelta spontanea del titolare o responsabile del trattamento. Nonostante la volontarietà nell'accesso, il contenuto di questa, e dunque i requisiti da rispettare, sono di natura cogente in quanto determinati sulla base del Regolamento[43]. Il fatto che la certificazione sia impostata sulle regole del GDPR comporta la non esaustività del sistema delle certificazioni rispetto ai controlli e all'assetto di monitoraggio delle autorità previsto dal Regolamento. Infatti, ai sensi dell'art. 42, par. 4 è lasciata impregiudicata ogni facoltà per l'Autorità Garante di contestare eventuali non conformità al Regolamento da parte del titolare o responsabile del trattamento certificato. Cionondimeno, l'asseverazione di un determinato trattamento da parte di un ente terzo permette comunque di comprendere, *prima facie,* la conformità dello stesso al Regolamento (ad esempio, certificando un prodotto o servizio prima della sua immissione nel mercato) e di acquisire esperienza e competenza rispetto alla scelta delle misure tecniche ed organizzative necessarie da implementare, caso per caso, per svolgere un trattamento di dati personali lecito.

Dato che le certificazioni ai sensi del GDPR appartengono alla forma legislativa della co-regolamentazione, il Regolamento non istituisce dei meccanismi di certificazioni, formalizza criteri o norme le quali incarichino che queste siano formate dalle autorità pubbliche europee o nazionali, ma prevede solamente che questi ultimi, e in particolare l'EDPB, la Commissione e le autorità di controllo nazionali, incoraggino l'instaurazione di meccanismi di certificazione della protezione dei dati che hanno l'obiettivo di attestare la conformità al regolamento. Essa può essere esercitata sia a livello nazionale che a livello europeo, e anzi il Regolamento prevede, in maniera coerente, che l'attività di incoraggiamento si eserciti soprattutto a livello dell'Unione[44]. Tuttavia, a fronte dell'assenza di spunti ulteriori dal dato normativo, la sfida principale dello strumento certificativo sembra essere non quella di architettare forme e procedure di co-regolamentazione, in quanto rimesse alla determinazione da parte degli operatori privati, quanto quella, più ardua, di valorizzarle nella quotidiana attività di applicazione e esecuzione delle regole.

[43] Cfr. A.R. POPOLI, *Codici di condotta e certificazioni*, *op.cit.*, 406; E. BELLISARIO, *Certificazioni di qualità e responsabilità civile*, *op.cit.*, 11-12. In dottrina, questo tipo di certificazioni sono definite come 'certificazione regolamentata', ossia strumenti di conformità il cui accesso è spontaneo, ma le regole del sistema sono fissate dalle autorità competenti e, come tali, hanno carattere cogente. La conformità a queste regole costituirebbe quindi una certificazione obbligatoria.

[44] Cfr. S. SILEONI, *I codici di condotta e le funzioni di certificazione*, *op. cit.*, 929.

Il meccanismo delle certificazioni esalta il ruolo dei soggetti privati, dal momento che la certificazione può essere rilasciata, oltre che dalle autorità indipendenti, da organismi appositamente accreditati. Tali organismi sono chiamati a verificare la conformità del trattamento a criteri approvati dalle autorità nazionali o dal Comitato, rilasciando, in caso di positivo riscontro, un'attestazione che può avere validità per massimo tre anni, con possibilità di rinnovo. Anche la fase costitutiva è sostanzialmente privatistica. Difatti, la certificazione, o il sigillo o marchio, dovranno essere sviluppati dagli enti ed organismi privati, secondo requisiti e criteri che dovranno poi essere approvati dalle varie autorità di controllo competenti.[45]

Il rafforzamento da parte del Legislatore europeo dei codici di condotta e degli strumenti di certificazione per il trattamento dei dati personali pare confermare che "*il diritto – che se ne abbia consapevolezza o no – è molto, ma molto più ampio ed esteso del diritto stabilito da un'autorità pubblica*"[46]. Come si è detto, la co-regolamentazione permette di garantire la commistione fra norme generali caratterizzate da un elevata obsolescenza tecnologica e norme tecniche, di produzione privata, capaci di essere modificare rapidamente e frequentemente, proprio in base agli sviluppi della tecnologia. Con questa tecnica normativa, quindi, il Legislatore permetterebbe di dare spazio alle istanze private all'interno del sistema regolativo. La promozione dello sviluppo di schemi di certificazione, sulla base di una determinazione legislativa, sarebbe rivolta a includere nuovi attori di un diverso sistema istituzionale in cui l'organo legislativo svolge il ruolo di cerniera sia rispetto al sistema delle fonti, sia nel rapporto tra questo sistema e la società[47].

Un ulteriore peculiarità da affrontare appartiene al piano definitorio. Il GDPR, infatti, non fornisce una definizione di certificazione, venendo la stessa espressa solamente nelle Linee Guida 1/2018. In queste ultime, l'EDPB mutuando la definizione dagli standard ISO, che considerano la certificazione come "*l'erogazione da parte di un organismo indipendente di garanzia scritta (un certificato) che il prodotto, il servizio o il sistema in questione soddisfano requisiti specifici*" o come "*un'attestazione da parte di un organo terzo relativa a prodotti, processi e servizi*"[48], ha definito la certificazione a norma degli artt. 42 e 43 GDPR come un attestazione di terza parte relativa ai trattamenti effettuati dal titolare del trattamento e dal responsabile del trattamento[49]. Sempre sul piano definitorio, il Regolamento fa riferimento a meccanismi di certificazione, marchi o sigilli di conformità, senza fornire una distinzione di questi, ma spesso utilizzandoli insieme o promiscuamente. Ciò, in realtà, è concettualmente errato,

[45] Cfr. *ivi*, 930;

[46] Cfr. A. BALDASSARRE, *Globalizzazione contro democrazia*, Roma-Bari, 2002, 21.

[47] Cfr. S. SILEONI, *I codici di condotta e le funzioni di certificazione*, *op. cit.*, 938; v. S. Rodotà, *intervento alla riunione interistituzionale sulla legislazione*, Palazzo Montecitorio, 21 giugno 1999, res. sten., 2. Per maggiori approfondimenti v. E. LACHAUD, *The General Data Protection Regulation and the rise of certification as a regulatory instrument*, in *Computer Law & Security Review*, 2018, vol. 34, 244-256, in Rete: *https://www.sciencedirect.com/science/article/abs/pii/S0267364917302121*.

[48] Mentre per attestazione si intenderebbe "*l'emissione di una dichiarazione, basata su una decisione successiva al riesame, da cui risulta che è stato dimostrato il rispetto dei requisiti specificati*".

[49] Cfr. EDPB, *Linee Guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione in conformità degli articoli 42 e 43 del Regolamento,* 2019, in Rete: *https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_it.pdf*.

oltre che confusionario; infatti, i marchi o i sigilli non sono altro che il simbolo grafico o il logo, la cui presenza dimostra l'esito positivo del procedimento di certificazione, rappresentando chiaramente al pubblico la conformità (presunta) al Regolamento del titolare o responsabile del trattamento aderente alla certificazione[50].

Le certificazioni, insieme ai codici di condotta, sono richiamati notevoli volte all'interno del GDPR; tuttavia, la loro disciplina effettiva è unitariamente prevista al Capo IV del Regolamento, all'interno della Sezione V, topograficamente consecutiva alle norme in materia di obblighi generali del titolare e responsabile del trattamento, rubricata "Codici di condotta e certificazioni", agli artt. 42 – "Certificazione", riguardante l'oggetto e gli aspetti procedurali dei meccanismi di certificazione, e 43 – "Organismi di Certificazione", che completa l'articolo precedente disciplinando la procedura di accreditamento.

Indagando il testo di questi articoli possono essere immediatamente evinti due elementi: da una parte, il sistema dei procedimenti di certificazione, concernente il processo di certificazione in senso stretto e quello di accreditamento; dall'altra, tutti i soggetti coinvolti nel sistema ideato dal Legislatore europeo.

Partendo dagli attori coinvolti nel 'processo' certificativo, il Regolamento individua: i titolari o responsabili del trattamento che possono aderire ad un meccanismo di certificazione, gli Organismi di Certificazione, le autorità di controllo nazionali, gli organismi nazionali di accreditamento designati in virtù del Regolamento (CE) n. 765/2008[51], l'EDPB, la Commissione UE e gli Stati membri. Pur non essendo esplicitato nella norma, un ulteriore soggetto da prendere in considerazione è lo *scheme owner,* cioè la persona fisica o giuridica che definisce i criteri e le procedure di certificazione[52].

Della Commissione e degli Stati membri si è già detto che il loro compito principale è quello di 'incoraggiare' l'istituzione di meccanismi di certificazioni della protezione dei dati. Accanto a tale incarico, tuttavia, alla Commissione sono stati riconosciuti ulteriori poteri di intervento, potendo adottare atti delegati finalizzati a stabilire o precisare i requisiti e le norme tecniche dei meccanismi di certificazione[53]

---

[50] Cfr. *ivi*, 9; L. BOLOGNINI, *Art. 42 – Certificazione*, in L. BOLOGNINI, E. PELINO, I. M. ALAGNA (a cura di), *Codice della Disciplina Privacy*, Milano, 2019, 296, ove l'a. fa preciso riferimento al principio interpretativo contenuto nel paragrafo 19 delle citate Linee Guida 1/2018, con cui si evidenzia che sigilli e marchi siano loghi o simboli la cui presenza indica che un processo di certificazione è avvenuto e che un organo indipendente ha esaminato la conformità, del soggetto a cui il marchio o sigillo è apporto, agli specifici requisiti previsti dalla certificazione ai quali si sommano i criteri di certificazione approvati dall'Autorità competente.

[51] Il Regolamento (CE) n. 765/2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti, fa parte di un progetto legislativo volto a garantire e favorire la libera circolazione dei prodotti nell'UE attraverso il rafforzamento della normativa sul riconoscimento delle norme tecniche nazionali e della vigilanza del mercato.

[52] Cfr. EDPB, *Linee Guida 1/2018*, *op. cit.*, 11. Sul suo ruolo vedasi *infra*.

[53] Cfr. art. 43, par. 8-9: "*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 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*".

Ritornando ai soggetti che possono aderire ai meccanismi di certificazione, l'art. 42, par. 2[54], presenta una peculiarità, discernendo titolari o responsabili del trattamento soggetti al Regolamento da quelli che, invece, ai sensi dell'art. 3[55], non lo sono. Da un lato, quindi, i soggetti sottoposti al Regolamento, possono aderire ai meccanismi di certificazione per dimostrare la propria conformità, conformando le loro attività al corretto trattamento dei dati personali. Agendo come fonti supplementari alla disciplina normativa, i criteri di certificazione aiuterebbero i destinatari del GDPR a comprendere meglio, in termini applicativi, la portata dei loro obblighi, tenendo conto del potenziale rischio del trattamento sui diritti e le libertà delle persone titolari dei dati[56]. Dall'altro lato, i soggetti estranei all'ambito di applicazione del Regolamento possono aderire a meccanismi, sigilli e marchi di certificazione al fine di dimostrare la previsione di garanzie adeguate al trasferimento transfrontaliero di dati personali. Una volta aderito alla certificazione, infatti, anche per questi soggetti terzi vige l'obbligo di applicare le stesse garanzie per la tutela dei diritti degli interessati.

Come si è avuto modo di menzionare precedentemente, nel processo di certificazione, accanto ai 'soggetti da certificare', sono coinvolti altri attori, ossia l'Organismo di Certificazione, l'autorità di controllo nazionale e l'organismo nazionale di accreditamento. Su di queste il Regolamento basa il sistema di valutazione della conformità disponendo un assetto gerarchico-piramidale fra queste entità, le quali, però, rimangono autonome e indipendenti l'una dall'altra. Proprio tali caratteristiche, insieme a quella della terzietà di questi organismi rispetto ai soggetti da certificare, rappresentano i requisiti essenziali per la tenuta e l'affidabilità del sistema co-regolativo basato sulle certificazioni.[57]

---

[54] Cfr. Art. 42, par. 2: "*Oltre all'adesione dei titolari del trattamento o 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*".

[55] In particolare, l'art. 3 GDPR definisce l'ambito di applicazione territoriale del regolamento, prevedendo che questo si applichi al "*al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione*", nonché rispetto al "*trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione"*. Per approfondimenti sull'ambito di applicazione territoriale v. P. GUARDA, G. BINCOLETTO, *Diritto comparato della privacy e della protezione dei dati personali*, Zenodo, 2023, 64, in Rete: *https://doi.org/10.5281/zenodo.7805085*; A. NERVI, *Il perimetro del Regolamento europeo: portata applicativa e definizioni*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I Dati Personali Nel Diritto Europeo*, Torino, 2019, p. 162-177.

[56] Cfr. S. SILEONI, *I codici di condotta e le funzioni di certificazione*, *op. cit.*, 931; considerando n. 77.

[57] Cfr. G.M. RICCIO, V. VITI, *Le "Certificazioni privacy" ed il Regolamento UE*, *op. cit*.

Del ruolo delle varie autorità pubbliche ed organismi privati coinvolti si sarà conto nei successivi paragrafi. Ciò nonostante, è necessario procedere ad una considerazione preliminare in merito al delicato rapporto tra questi enti e i soggetti da certificare. Il rischio riscontrabile nel sistema previsto dal GDPR, infatti, è che i grandi operatori privati possano avere la capacità di influenzare coloro che intendano sviluppare schemi di certificazione o gli enti preposti alla valutazione della conformità di un trattamento ai criteri della certificazione[58]. In queste, ed altre, circostanze i rapporti fra i soggetti coinvolti nel processo di certificazione devono essere improntati ad assoluta trasparenza e correttezza[59], al fine di garantire il rispetto del Regolamento, nonché dei diritti e libertà assegnati agli interessati del trattamento, e soprattutto di non ledere l'affidamento che questi ultimi possono riporre nello strumento certificativo e in ciò che rappresenta.

Come pocanzi si accennava, gli artt. 42 e 43 GDPR descrivono tutto il procedimento relativo alle certificazioni. Quest'ultimo è in realtà scomponibile in una serie di 'fasi' che possono coinvolgere differentemente i soggetti precedentemente richiamati, ma che, tuttavia, è possibile riassumere in uno schema 'base', utile a fornire una preliminare immagine di come operino, in via semplificata, le certificazioni nel GDPR.

La prima fase è quella di creazione dei meccanismi di certificazione, e, in particolare, della determinazione dei criteri, delle modalità di verifica e della successiva convalida dello schema da parte di un'autorità nazionale di controllo o dell'EDPB[60].

La seconda fase concerne l'accreditamento degli Organismi di Certificazione (o OdC). Questi organismi sono coloro che potranno rilasciare le certificazioni, verificando la conformità dei soggetti da certificare allo schema precedentemente approvato[61]. Tali enti non necessariamente coincidono con il soggetto che sviluppa il meccanismo di certificazione e richiede l'approvazione dello stesso da parte dell'autorità di controllo competente, dovendo in tal caso dimostrare le proprie conoscenze e competenze rispetto al meccanismo di certificazione che poi si andrà ad attribuire. Quest'ultimo non rappresenta l'unico requisito che tali soggetti devono avere per svolgere le loro attività, ma sarà necessario che questi dimostrino, mediante una procedura di accreditamento davanti alle autorità competenti, di essere soggetti indipendenti, non in conflitto di interessi, competenti in materia di protezione dei dati (e non solo sullo specifico schema

[58] Il rischio, infatti, è che nel primo caso si andrebbero a predisporre dei criteri insufficienti rispetto alle garanzie richieste dalla normativa, mentre nel secondo potrebbe permettersi il rilascio delle certificazioni sulla base di valutazioni fumose o scorrette, o comunque in situazioni di conflitto di interessi.

[59] Proprio il GDPR richiama il concetto di trasparenza come elemento fondamentale del sistema predisposto in tema di certificazioni. Infatti, l'art. 42, par. 3 prevede che la certificazione, oltre ad essere volontaria, dev'essere accessibile mediante una procedura trasparente, mentre l'art. 43, par. 2, lett. d), in tema di requisiti di accreditamento degli OdC prevede che questi debbano istituire "*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*".

[60] Cfr. art. 42, par. 1-4-5.

[61] Cfr. art. 43, par. 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*".

di certificazione) e che abbiano formalizzato apposite procedure per il processo di rilascio della certificazione[62].

La terza e quarta fase riguardano rispettivamente la verifica del soggetto da certificare e l'eventuale rilascio della certificazione da parte degli OdC accreditali o direttamente dall'autorità garante competente [63] e la supervisione successiva del soggetto certificato ad opera degli OdC e delle autorità di controllo nazionali[64].

3 La creazione di uno schema di certificazione ai sensi del GDPR

Come si è avuto modo di osservare, alla quinta sezione del quarto capo sono regolate le certificazioni ai sensi del GDPR. In particolare, l'art. 42 prevede che "*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".* Primo elemento che risalta dalla lettura del precedente canone è che il Regolamento fa riferimento a "*meccanismi di certificazione"*. Il termine, infatti, è stato usato al fine di sviluppare un contesto in cui siano ammissibili una pluralità di schemi certificativi rivolti a soddisfare anche esigente differenti l'uno dall'altro. Proprio l'art. 42 GDPR dispone che nella previsione di tali meccanismi debbano essere tenuti in conto gli interessi ed esigenze specifiche delle PMI[65], evidenziando, in questo modo, come una differenziazione non sia necessaria solamente a livello dimensionale, ma, indirettamente, soprattutto a livello della portata

[62] Cfr. art. 43, par. 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 la revoca 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 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*".

[63] Cfr. art. 42, par. 6-7: "6. *Il titolare del trattamento o il responsabile del trattamento che sottopone il trattamento effettuato al meccanismo di 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 criteri 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 criteri per la certificazione*".

[64] Cfr. art. 43, par. 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*".

[65] Cfr. L. BOLOGNINI, *Art. 42 – Certificazione*, in *Codice della disciplina privacy*, *op.cit.*, 295.

delle attività e trattamenti svolti da un'impresa. Certamente è ragionevole prevedere che una grande o media impresa svolga molti più trattamenti di una piccola impresa, ma è anche plausibilissimo che una start-up innovativa svolga trattamenti quantitativamente e qualitativamente superiori, o più 'sensibili' rispetto alle prime due.

Ecco, pertanto, che di tali circostanze dovranno tener conto coloro che sviluppano i meccanismi di certificazione, arrivando, quindi, all'interrogativo principale. Chi è che sviluppa i suddetti meccanismi?

L'art. 42, al primo paragrafo da solamente conto che gli Stati membri, le autorità di controllo, il comitato e la Commissione 'incoraggino' l'adozione delle certificazioni e non che queste siano direttamente coinvolte nel loro sviluppo; per di più, oltre agli Organismi di Certificazione, ai titolari e responsabili del trattamento, all'autorità nazionale di controllo e all'EDPB non vengono menzionati ulteriori soggetti a cui potrebbe essere demandato la creazione di meccanismi di certificazione. Pertanto, a fronte della mancanza di prescrizioni specifiche, nonché in raccordo con le indicazioni fornite dall'art. 40, par. 2, è da ritenersi che ogni ente, associazione, od organismo privato, che sia in qualunque modo correlato alla materia della protezione dei dati personali, in ragione delle proprie competenze, abilità o conoscenze, possa procedere alla produzione di un meccanismo di certificazione. Anche se dal Regolamento o nelle varie Linee Guida dell'EDPB emergerebbe l'idea per cui sarebbero gli stessi OdC a realizzare le certificazioni per poi approvarle e vedersi accreditati sulla base di esse, questa visione non è la sola ammessa. Può ben essere possibile, infatti, che la certificazione sia creata da un soggetto terzo agli OdC, il quale poi consentirà, con licenza, a questi ultimi di assegnare le certificazioni. A fronte di questa distinzione dei ruoli interpretabili dagli attori privati, la prassi ha denominato quest'ultimo come lo *scheme owner*: nel processo di certificazione, egli si occuperà della definizione dei criteri e muoverà l'iniziativa per l'approvazione degli stessi verso l'autorità di controllo.

Infine, anche se si è detto che i meccanismi di certificazioni possono essere istituiti dai soggetti privati, tale lettura sarebbe, in realtà, imprecisa. Infatti, come si vedrà successivamente, il Regolamento in nessun punto impedisce alle autorità di controllo nazionali, o ad altri organismi di diritto pubblico[66], di intervenire per la definizione di una certificazione ai sensi del GDPR, essendo, eventualmente, rimessa alla legislazione degli Stati membri operare una scelta più specifica sul punto. D'altronde, data la genericità del compito di tali organi di 'incoraggiare' l'istituzione di meccanismi per la protezione dei dati, può ben ipotizzarsi un'interpretazione più o meno ampia dello stesso.

[66] In relazione agli organismi di diritto pubblico, si tenga conto che comunque questi hanno una definizione ampia ed elastica, in quanto necessaria a soddisfare l'applicazione dei vari principi contenuti nei trattati. Organismo di diritto pubblico è, infatti, qualsiasi organismo, anche in forma societaria, istituito per soddisfare specificatamente esigenze di interesse generale, aventi carattere non industriale o commerciale, che sia dotato di personalità giuridica e la cui attività sia finanziata in modo maggioritario dallo Stato, dagli enti pubblici territoriali o da altri organismi di diritto pubblico; oppure la cui gestione sia soggetta al controllo di questi ultimi, oppure, da ultimo, il cui organo d'amministrazione, di direzione o di vigilanza sia costituito da membri dei quali più della metà sia designata dallo Stato, dagli enti pubblici territoriali o da altri organismi di diritto pubblico. Per approfondire v. G. STRAZZA, *Organismo di diritto pubblico*, in *l'Amministrativista*, 2020, in Rete: *https://lamministrativista.it/bussola/organismo-di-diritto-pubblico*.

3.1 Ambito di applicazione e oggetto della certificazione (c.d. *target of evalutation*)

L'art. 42, par. 1, come visto, incoraggia l'istituzione di meccanismi di certificazione "*allo scopo di dimostrare conformità al presente regolamento dei trattamenti effettuati dai titolari di trattamento e dai responsabili di trattamento"*.

Con questo inciso, insieme a quanto contenuto nel considerando n. 100, si individua l'ambito di applicazione delle certificazioni ai sensi del GDPR, ossia ai soli trattamenti effettuati dai titolari e responsabili del trattamento. La limitazione all'ambito di applicazione è redatta sulla base di due principi, uno soggettivo, ossia il riferimento esclusivo a titolari e responsabili del trattamento, e l'altro oggettivo.

Per quanto riguarda l'ambito soggettivo di applicazione, l'art. 42 prende in considerazione esclusivamente titolari e responsabili del trattamento. Ciò comporta che non potrà ricorrere a meccanismi di certificazione per lo svolgimento delle proprie attività il *Data Protection Officer*, il quale potrà comunque certificare le proprie competenze nella materia della protezione dei dati personali ma con altro strumento diverso dalle certificazioni ai sensi del GDPR[67]. A fronte della riserva ai soli titolari e ai responsabili (nonché *sub*-responsabili) del trattamento, è ragionevole ipotizzare situazioni in cui un titolare del trattamento, che non faccia ricorso a certificazioni, abbia nominato uno o più responsabili del trattamento che ricorrano invece a questi meccanismi per rafforzare la fiducia dei titolari stessi, soprattutto rispetto a responsabili 'esterni', i quali saranno, probabilmente, i più incentivati a adottare questo strumento[68].

Per quanto riguarda l'ambito oggettivo di applicazione, ossia che cosa possa essere certificato ai sensi del Regolamento, l'art. 42, infatti, fa generico riferimento ai "*trattamenti"* di dati personali e alla possibilità che le certificazioni possano essere utilizzate per dimostrare la conformità del medesimo al Regolamento.

Come sottolineato dalla dottrina, a differenza dei codici di condotta, i quali sono limitati a particolari categorie di trattamenti o parti di essi, le certificazioni hanno un raggio applicativo più vasto potendo concernere ogni possibile trattamento di dati personali. Ciò che è necessario, come individuato dal Comitato nelle Linee Guida 1/2018, è che nella valutazione del trattamento si tenga conto di tre elementi fondamentali, cioè i dati personali trattati (in quanto determinano l'ambito di applicazione materiale del Regolamento), i sistemi tecnici o le infrastrutture utilizzate per trattare i dati personali (quali sintomatici delle misure tecniche implementate) e i processi e le procedure relative al trattamento (per le corrispondenti misure organizzative previste)[69]. Ognuno di questi è fondamentale ai fini della progettazione tanto delle procedure, quanto dei criteri di certificazione; inoltre, la misura di cui si dovrà tener conto dei tre elementi

[67] Come illustrato nel precedente capitolo, tuttavia, la certificazione del DPO non costituisce una certificazione di un prodotto, processo o servizio, ma la mera attestazione delle competenze di una determinata persona (es. la norma UNI 11967:2017).

[68] Cfr. D. POLETTI, M.C. CAUSARANO, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione, op.cit.*, 395 ss. L'autrice, inoltre, sottolinea come la certificazione appaia particolarmente adeguata all'operatività della tecnologia *blockchain* o ai servizi di *cloud computing*.

[69] Cfr. EDPB, *Linee Guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione*, *op. cit*., 17.

menzionati dovrà variare a seconda dell'oggetto della certificazione e dei vari fattori che possono influire sul trattamento di dati personali[70].

Sulla base di tali considerazioni l'EDPB ha ritenuto che l'ambito di applicazione delle certificazioni GDPR si estenda proprio ad ogni trattamento o insieme di trattamenti. Da questo punto di vista, la flessibilità mostrata dal Regolamento per l'ambito di applicazione delle certificazioni è bilanciata dalla cornice entro la quale le certificazioni devono operare, lasciando alle associazioni di categoria private e agli Stati membri, per il tramite delle autorità di controllo, contestualizzare l'ambito di applicazione dello schema di certificazione. Rispetto a tale situazione, ad esempio, i processi di *governance* interni, intesi come misure organizzative, potrebbero rientrare nell'ambito di applicazione di una certificazione, in quanto parti integranti di un trattamento[71].

In ogni caso, il Comitato specifica che per valutare la conformità ai criteri di certificazione è necessario indicare il perimetro applicativo, attraverso cui, poi, parametrare i criteri di certificazione e le modalità di valutazione delle misure tecniche ed organizzative previste per un trattamento[72]. Tale perimetro, tuttavia, non dev'essere eccessivamente limitato dalla previsione di criteri tecnici od organizzativi che possano influire sul campo di applicazione tanto da escludere applicazioni informative o misure di *governance* non prese in considerazione dalle certificazioni.

Infine, un ulteriore elemento caratteristico della certificazione, distinto dal campo di applicazione della stessa, è il suo oggetto, detto anche *target of evalutation*. Con tale termine si identifica il singolo o i plurimi trattamenti di dati personali che rientrano nel campo di applicazione della certificazione. L'ambito applicativo di una certificazione può già ben definire quello che sarà il suo oggetto, tuttavia, una descrizione specifica del singolo oggetto di un meccanismo di certificazione è necessaria per garantire l'affidabilità della certificazione. In particolare, come riconosciuto dall'EDPB, dovranno essere descritti chiaramente "*i trattamenti inclusi nell'oggetto della certificazione e quindi gli elementi chiave, ossia quali dati, processi e infrastrutture tecniche saranno sottoposti alla valutazione e quali no*"[73]. Per spiegare il concetto di *target of evaluation* pone l'esempio di una banca, con un proprio sito internet, che intende certificare il proprio sistema di *log-in*. Ecco, quindi, che i trattamenti di dati personali coinvolti durante il procedimento di autenticazione per l'accesso al portale bancario costituirà

[70] Cfr. *ibidem.* Sul punto, l'EDPB individua quattro diversi fattori significativi che possono influire sul trattamento: 1) l'organizzazione e la forma giuridica del titolare o responsabile del trattamento; 2) il personale coinvolto nel trattamento o nei trattamenti; 3) la descrizione tecnica degli elementi oggetto della valutazione; 4) l'infrastruttura informatica complessiva a sostegno del trattamento. Quest'ultima, in particolare, dev'essere intesa come l'intero comparto di elaborazione dei dati tra cui sistemi operativi, macchine virtuali, *database*, sistemi di autenticazione e autorizzazione (anche biometrici), *router*, *firewall*, sistemi di archiviazione e *cloud-storage*.

[71] Cfr. EDPB, *Linee Guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione*, *op. cit*., 18.

[72] Limitare la certificazione ad uno specifico caso d'uso è necessario in quanto, in un dato trattamento, la conformità dell'utilizzo di una data infrastruttura informatica o delle misure organizzative previste dipendono dalle categorie e dalla quantità dei dati coinvolti nel trattamento, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, oltre che dei rischi per i diritti e le libertà degli interessati.

[73] Cfr. *ivi*, 19.

l'oggetto della certificazione ai sensi del GDPR, la quale potrà anche avere un ambito applicativo più ampio, quale ad esempio tutti i trattamenti che necessitino di un grado elevato di sicurezza, ma che, nel caso della banca, l'oggetto è incentrato solamente nel processo di *log-in* e nei trattamenti ad esso connessi. A fronte di tale esempio, si può individuare l'oggetto di una certificazione quale quell'insieme di trattamenti, riferito ad un prodotto o servizio, che siano tra loro collegati e che abbiano, nella loro molteplicità, un senso compiuto e unitario[74]. Data, ovviamente, la complessità nell'individuare i trattamenti oggetto di valutazione, l'identificazione di questa attività è un elemento chiave nella procedura di certificazione in quanto sarà anche il primo fattore che verrà valutato dagli OdC.

Al fine di facilitare la comprensione dei trattamenti che possono rientrare nell'ambito di una certificazione, i titolari del trattamento e gli *auditor* dell'OdC possono utilizzare uno strumento previsto dal GDPR, ossia il Registro dei trattamenti. Ove correttamente stilato dal titolare o responsabile del trattamento, questo permette di individuare i singoli trattamenti svolti da questi ultimi, potendo individuare, fra questi, anche quel trattamento oggetto di valutazione della certificazione. Tuttavia, non è detto che solo un singolo *record* del Registro dei trattamenti costituisca il *target of evaluation* di una certificazione. Infatti, come si è precedentemente accennato, e come ribadito dal *Board*, possono rientrare nell'oggetto anche trattamenti plurimi, i quali siano reciprocamente connessi[75]. Infine, sempre rispetto al Registro dei trattamenti, non è neanche detto che un singolo *record* di quest'ultimo possa corrispondere, come minimo, all'oggetto di valutazione. Il singolo trattamento descritto nel Registro, infatti, può essere più esteso rispetto a quanto certificabile, dovendo necessariamente sezionare l'attività di trattamento complessiva inserita in Registro in più 'parti'.

In conclusione, l'individuazione dei trattamenti inclusi nel *target of evaluation* della certificazione rappresenta un difficile attività strettamente legata alla previa definizione, da parte del soggetto che intende certificarsi, dell'organizzazione delle attività di trattamento dei dati. Oltre ciò vi è da tener in conto, infine, che il singolo oggetto della certificazione dev'essere significativo rispetto al messaggio o allo slogan della certificazione, fornendo una rappresentazione di quello che si è andati a valutare, al fine di non sviare l'utente-interessato che si interfaccia al prodotto o servizio il cui trattamento è certificato[76].

---

[74] Cfr. L. BOLOGNINI, intervento presentato al seminario *Il meccanismo delle certificazioni con il GDPR – Il primo sigillo europeo per la protezione dei dati: la certificazione di Europrivacy*, 22 novembre 2022, in Rete: *https://www.federprivacy.org/attivita/webinar-sul-meccanismo-delle-certificazioni-con-il-gdpr-e-il-primo-sigillo-europeo-sulla-protezione-dei-dati.*

[75] Cfr. EDPB, *Linee Guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione*, *op. cit*., 19, ove il Comitato evidenzia come nella descrizione dell'oggetto della certificazione debbano essere sempre presi in considerazione e descritti le eventuali interfacce con altri processi, e quindi eventuali trattamenti connessi con quello oggetto di valutazione.

[76] Cfr. M. GRAFENSTEIN, *Co-Regulation and the Competitive Advantage in the GDPR: Data protection certification mechanisms, codes of conduct and the "state of the art" of data protection-by-design*, in G. GONZÁLEZ-FUSTER, R. BRAKEL, P. DE HERT (a cura di), *Research Handbook on Privacy and Data Protection Law*, 2019, 21-22, in Rete: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=33 36990*.

3.2 I criteri di certificazione e l'approvazione del meccanismo di certificazione

Ai sensi dell'art. 42, par. 5, il rilascio della certificazione è subordinato al possesso, del trattamento, di determinati requisiti di carattere tecnico ed organizzativo che devono essere implementati dal titolare o dal responsabile del trattamento affinché il marchio o sigillo sia rilasciato. Questi requisiti si sostanziano nei criteri di certificazione, ossia nei parametri di *audit* che gli Organismi di Certificazione utilizzeranno per verificare la *compliance* del soggetto da certificare e a cui titolare o responsabile del trattamento, che intendono aderire ad uno schema di certificazione, devono adeguarsi.

Compre previsto dal citato articolo, perché un meccanismo di certificazione possa essere rilasciato, l'autorità di controllo competente o l'EDPB dovranno approvarne i relativi criteri. Al di fuori di questo inciso, il Regolamento nulla dice in merito ai criteri di certificazione nonché rispetto alle modalità con cui individuarli e redigerli per un determinato schema. Ciò rappresenta la problematica principale sul punto; infatti, se per le procedure di certificazione, nonché i relativi criteri, la disciplina regolativa è ravvisabile negli artt. 42-43 GDPR, non altrettanto si può dire per i criteri di certificazione, determinando una forte incertezza nell'effettiva possibilità di sviluppare meccanismi di certificazione.

A fronte di tale incertezza, il Comitato Europeo per la protezione dei dati personali è intervenuto con le citate Linee Guida 1/2018 per chiarire le modalità di identificazione dei criteri di certificazione in conformità degli artt. 42 e 43, nonché della relativa procedura di approvazione da parte delle autorità pubbliche[77].

Con il presente documento, l'EDPB ha affermato che i criteri relativi alle certificazioni devono riflettere i requisiti e principi del GDPR. Il Regolamento già fornisce alcuni criteri di valutazione che possono essere sfruttati per certificare la conformità del trattamento. I criteri di certificazione dovranno essere tratti, di conseguenza, dagli artt. 5 e 6, relativamente ai principi del trattamento e alle condizioni che ne disciplinano la liceità, dai diritti degli interessati previsti *ex* artt. 12-23, dagli obblighi di sicurezza e dalla procedura di segnalazione dei *data breach* prevista negli artt. 32 e 33, dai principi della *privacy by design* e *by default* ai sensi dell'art. 25, nonché da quelli derivanti dalla DPIA *ex* art. 35. Dopotutto, tali oneri fanno tutti parte del principio di *accountability* verso cui le certificazioni devono essere rivolte[78].

Lo sviluppo dei criteri di certificazione dovrebbe quindi concentrarsi sulla verificabilità, rilevanza e idoneità di tali elementi ai fini della dimostrazione della conformità al Regolamento. Tenendo poi conto dell'applicazione pratica delle certificazioni quali mezzi di dimostrazione del principio di *accountability*, i criteri di certificazione per esso definiti devono essere chiari e comprensibili sia rispetto all'organizzazione che intende certificarsi, sia rispetto ai terzi-interessati, proprio per

[77] È proprio l'EDPB a qualificare quale obiettivo primario delle linee guida quello di "*identificare requisiti e criteri generali che possano applicarsi a tutti i tipi di meccanismi per le certificazioni rilasciate in conformità degli articoli 42 e 43 del regolamento*".

[78] Cfr. L. BOLOGNINI, *Art. 42 – Certificazione*, in *Codice della disciplina privacy*, *op.cit.*, 296. Per approfondire il tema delle norme i cui obblighi possono essere dimostrati con l'adesione ad una certificazione ai sensi del GDPR, v. E. LACHAUD, *Accountability and Certification in the GDPR*, 2021, in Rete: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3948093*.

consentire a questi ultimi di valutare rapidamente, ed efficacemente, il livello di protezione dei dati offerto dai vari prodotti e servizi[79].

Data l'ampia libertà tracciata nelle norme sopramenzionate rispetto agli adempimenti del titolare o responsabile del trattamento, la misura con cui i criteri di certificazione traggono ispirazione dai principi e considerazioni del GDPR può significativamente variare a seconda della portata della certificazione, ossia del settore e del tipo di operazioni di trattamento che vengono certificate, nonché in ragione della dimensione dell'organizzazione dei soggetti che devono essere certificati[80]. Sulla base di questi ultimi elementi, infatti, la misura e la portata dei criteri di certificazione può variare notevolmente, contribuendo altresì a definire l'ambito di applicazione dei meccanismi certificativi medesimi.

Rispetto alla definizione dei criteri di certificazione le Linee Guida 1/2018 elencano una serie di caratteristiche generali di cui è necessario tener conto per lo sviluppo e successiva approvazione degli stessi. In particolare, i criteri di certificazione dovranno:

- essere uniformi e verificabili;
- specificare i propri obiettivi e le modalità attuative per raggiungerli, in modo tale da poter essere sottoposti a controlli volti ad agevolare la valutazione dei trattamenti a norma del Regolamento generale sulla protezione dei dati;
- essere pertinenti rispetto al pubblico a cui si rivolgono (ossia pertinenti riguardo ai rapporti B2B, B2C o B2G);
- tenere conto di eventuali altre norme (sia legislative che di prassi, quali le norme ISO) e laddove opportuno essere interoperabili con le stesse[81];
- essere flessibili e scalabili in modo da applicarsi a organizzazioni di diverso tipo e dimensione, comprese le micro, piccole e medie imprese;
- essere adattabili in ragione dei diversi contesti, settori e/o Stati membri al fine di allargare il possibile *target of evaluation* rientrante nell'ambito di applicazione della certificazione;
- corrispondere alla dichiarazione (messaggio o significato) determinata dall'apposizione del sigillo o marchio della dichiarazione e soddisfare le aspettative create dalla stessa. Anche la denominazione di un meccanismo di certificazione può già identificarne l'ambito di applicazione e, quindi, rappresentare con chiarezza agli interessati quali effetti essa potrà avere sul trattamento dei propri dati personali[82].

---

[79] Cfr. EDPB, *Linee Guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione*, *op. cit*., 17.

[80] D'altronde, proprio l'art. 42 fa riferimento al fatto che debbano essere tenuti in considerazione gli interessi delle micro, piccole e medie impese, e questo non può che essere fatto mediante una differente calibratura dei criteri di certificazione rispetto alla platea di soggetti che si intenderà certificare. Banalmente, un'impresa manifatturiera che tratti i dati dei propri clienti e fornitori mediante terminali informatici non sarà interessata ad una certificazione i cui criteri sono rivolti alla protezione di dati sanitari o biometrici, ma eventualmente ad una certificazione che attesti la conformità del trattamento di dati diversi rispetto a quelli indicati nell'art. 9 GDPR.

[81] Come si illustrerà *infra* le certificazioni ai sensi del GDPR possono produrre effetti anche rispetto alle ulteriori regole normative europee in tema di digitale e in cui siano coinvolti dati personali.

[82] Cfr. EDPB, *Linee Guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione*, *op. cit*., 22-24.

Tutti questi elementi devono essere parimenti presi in considerazione dall'autorità di controllo per l'approvazione dei criteri di certificazione a norma dell'art. 42, par. 5. La flessibilità lasciata agli operatori per lo sviluppo di variegati criteri di certificazione potrebbe determinare notevoli difficoltà ai vari Garanti europei per la valutazione di appropriatezza dei criteri rispetto alle norme del Regolamento. Inoltre, potrebbero svilupparsi prassi differenti fra le varie autorità garanti europee, pregiudicando l'armonizzazione della disciplina in tema di certificazioni. È per tale ragione che l'EDPB, nelle Linee Guida 1/2018, ha fornito, nel relativo allegato, una serie di orientamenti mirati a garantire un approccio armonizzato nella valutazione dei criteri ai fini dell'approvazione. Dopotutto, per approvare i criteri di certificazione un'autorità di controllo dovrebbe avere una comprensione chiara di quanto aspettarsi da questa, soprattutto nei termini di ambito di applicazione, possibili *targets of evalutation* e contenuti e verifiche per la dimostrazione di conformità al Regolamento. Nell'allegato alle Linee Guida, sono, quindi, state inserite una serie di differenti quesiti che l'autorità nazionale di controllo deve porsi per valutare la 'conformità' della certificazione rispetto ai principi previsti dal Regolamento e dalle linee guida[83].

Al fine di una migliore comprensione, viene inoltre previsto che per valutare la corretta predisposizione dei criteri di certificazione, deve essere fornito un caso d'uso. Ad esempio, la conformità dell'uso di una determinata infrastruttura informatica, invece di un'altra, dipende dalle categorie di dati da elaborare per cui l'infrastruttura è progettata. Inoltre, le misure organizzative possono variare in base alle categorie e quantità di dati e dall'infrastruttura tecnica utilizzata per l'elaborazione dei dati, tenendo conto della natura, dell'ambito, del contenuto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà degli interessati[84]. Fornire un caso d'uso permetterebbe di circostanziare meglio sia l'ambito di applicazione dei meccanismi della certificazione, sia la correttezza dei criteri *ivi* previsti. Pertanto, di tali elementi si dovrà dar conto all'autorità nazionale di controllo in sede di approvazione dei criteri di certificazione.

3.3 La circolazione delle certificazioni nel Mercato Unico Europeo: la Certificazione comune e il Sigillo europeo per la protezione dei dati personali

Il meccanismo di certificazione, e i relativi criteri, possono essere approvati non solo dall'autorità nazionale competente, ma anche dal Comitato Europeo per la protezione dei dati personali. Ai sensi dell'art. 42, par. 5 e dell'art. 64, par. 1, lett. c), infatti, l'EDPB può approvare la certificazione ad essa proposta dallo *scheme onwer* attribuendole valore sovrannazionale quale Sigillo europeo per la protezione dei dati personali[85].

[83] Cfr. *ivi,* 24 *ss*.

[84] Cfr. *ivi*, 18, paragrafi 56-57.

[85] Cfr. art. 42, par. 5: "*Ove i criteri siano approvati dal comitato, ciò può risultare in una certificazione comune, il sigillo europeo per la protezione dei dati.*"; art. 64, par. 1, lett. c): "*approvare i requisiti per l'accreditamento di un organismo ai sensi dell'articolo 41, paragrafo 3, di un organismo di certificazione ai sensi dell'articolo 43, paragrafo 3, o i criteri per la certificazione di cui all'articolo 42, paragrafo 5*".

L'attribuzione di valenza sovrannazionale alle certificazioni è data principalmente dalla capacità e dallo scopo dei criteri di certificazione di essere un comune denominatore fra i vari ordinamenti, risultando, di conseguenza, applicabili su scala comunitaria. Con l'adozione di una certificazione comune si consentirebbe di fissare degli *standard* condivisi tra i diversi Stati membri senza necessariamente sacrificare le specifiche esigenze di ciascuno di essi[86].

Al fine di soddisfare le richieste di certificazione su scala europea, i criteri di certificazione dovranno essere particolarmente flessibili, soddisfacendo tanto le esigenze comuni europee, quanto quelle specifiche richieste nei vari Stati membri. Di conseguenza, questi ultimi, proprio perché devono fungere da certificazione comune, oltre a rispettare la legislazione europea, dovranno essere adattabili alle normative settoriali nazionali[87].

Lo scopo della creazione del Sigillo europeo è consentire alle organizzazioni di possedere un tratto distintivo riconoscibile nei diversi Stati membri dell'Unione. Tale finalità attribuisce al ruolo del Sigillo europeo enormi potenzialità, offrendo un marchio che possa generare fiducia relativamente al trattamento dei dati personali valido in tutta Europa, frutto di una procedura trasparente con criteri affidabili, con la supervisione e garanzia fornita da una terza parte indipendente che garantisce immediata visibilità della conformità ai principi del Regolamento. Il Sigillo, quindi, racchiude un marchio di fiducia il quale attesta che un prodotto o un servizio è stato controllato da esperti indipendenti e approvato da un'autorità di certificazione imparziale, sulla base di criteri asservati dall'EDPB, ossia dal soggetto più autorevole ad interpretare la disciplina sul trattamento dei dati personali, garantendo affidabilità attraverso la promozione della protezione degli interessati e offrendo un potenziale vantaggio in termini di marketing per i prodotti o servizi certificati.[88]

Data l'importanza dello strumento l'EDPB è intervenuto diverse volte sul punto, attraverso la pubblicazione di documenti e Linee Guida che potessero aiutare a comprendere efficacemente le condizioni riferite al Sigillo europeo per la protezione dei dati e il procedimento operativo necessario per l'approvazione. Proprio quest'ultimo è stato oggetto di due documenti del Comitato, il quale ha compiutamente disciplinato a procedura per l'approvazione da parte dello stesso di criteri di certificazione validi nell'intera UE[89].

Partendo dalla fase di presentazione, il titolare di schemi di certificazione dovrà presentare i criteri di certificazione all'autorità competente per il luogo ove si colloca la

---

[86] Cfr. F. PEZZA, *Art. 42 – Certificazioni*, in E. Belisario, G.M. Riccio, G. Scozza (a cura di), *GDPR e Normativa Privacy*, Milano, 2020, 479.

[87] Cfr. EDPB, *Linee Guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione*, *op. cit*., 15-16. Sul punto, il Comitato pone l'esempio di una scuola internazionale, la quale ha sede in uno Stato membro "A" che intende certificare un proprio trattamento sulla base di uno schema di certificazione a livello europeo che, però, viene fornito da un OdC avente sede in uno Stato membro "B". In questo caso, quindi, i criteri per il sigillo dovranno tener conto delle regolamentazioni relative alle scuole e al trattamento di dati personali di minori applicabili nello Stato membro "A" e "B".

[88] Cfr. L. BOLOGNINI, *Art. 42 – Certificazione*, in *Codice della disciplina privacy*, *op.cit.*, 297.

[89] Cfr. EDPB, *Documento del Comitato europeo per la protezione dei dati sulla procedura di approvazione da parte del Comitato di criteri di certificazione riferiti a una certificazione comune, il sigillo europeo per la protezione dei dati*, 2020, in Rete: *https://edpb.europa.eu/our-work-tools/our-documents/procedure/edpb-document-procedure-approval-certification-criteria-edpb_it*.

sede di quest'ultimo, ovvero all'autorità competente per il luogo ove sia presente la sede principale dell'OdC che gestisce lo schema. A fronte della presentazione del progetto dei criteri, l'autorità di controllo esaminerà quest'ultimo al fine di garantire che soddisfi i requisiti del Regolamento. Questa preliminare analisi si pone come primo di una serie di filtri che, in caso di esito negativo, bloccano il procedimento di verifica dei criteri da parte del Comitato. Ove, invece, questa verifica di ammissibilità abbia esito positivo, l'autorità di controllo avvierà una procedura di cooperazione informale rivolta a coinvolgere tutte o parti delle altre autorità di controllo nazionali dell'Unione, i quali potranno assistere alla successiva fase di verifica. Particolare è il ruolo dei co-revisori, ossia dei membri dei Garanti nazionali europei che avranno il compito di assistere l'autorità di controllo competente nella valutazione del progetto di criteri, potendo anche formulare osservazioni. In questa fase, l'autorità di controllo competente, i co-revisori e le altre autorità avranno il compito di accertare l'accettabilità tecnica dei criteri di certificazione e che questi tengano adeguatamente conto della legislazione nazionale dei vari Stati membri. In queste fasi di controllo informale, è concesso allo *scheme owner* di emendare i criteri sulla base delle osservazioni delle autorità di controllo ovvero di formulare egli stesso delle osservazioni sui rilievi delle autorità.

Al termine della fase di cooperazione informale, l'autorità di controllo competente dovrà decidere se presentare o meno il progetto di criteri di certificazione al Comitato per l'approvazione formale. L'EDPB conoscerà il merito dei criteri solo ove questo passi il vaglio del Garante nazionale competente. In caso di esito positivo, il progetto sui criteri e la documentazione relativa saranno trasmetti al *Board* il quale avrà otto settimane (prorogabili di ulteriori sei) per decidere, con parere, sulla convalida o meno dei criteri[90]. Ove il parere sia positivo, e i criteri approvati, l'autorità di controllo competente comunica al titolare della certificazione l'esito e inoltra al Comitato tutti i documenti necessari per la pubblicazione della certificazione nell'apposito registro pubblico. In caso di esito negativo, invece, l'autorità di controllo potrà decidere di presentare nuovamente i criteri all'EDPB o di avviare, invece, una nuova fase di cooperazione informale per valutare gli aggiustamenti necessari da fare al meccanismo di certificazione.

4 Gli Organismi di Certificazione: il loro ruolo nel processo di certificazione

Come precedentemente evidenziato, l'art. 42, paragrafo 5 del Regolamento prevede che: "*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. […]*", riflettendo che la certificazione rilevante ai sensi del GDPR è solo quella rilasciata dagli appositi Organismi di Certificazione previsti dall'art. 43 o dall'autorità di controllo competente.

Come si avrà modo di descrivere, il sistema è definito in modo tale che tutto il meccanismo sia governato dall'autorità garante, quale ente che approva gli schemi,

[90] Cfr. *ivi*, 6, Tale parere terrà sempre conto di quanto enunciato in precedenti pareri sulla stessa materia, al fine di garantire la coerenza.

attribuisce le certificazioni e monitora il rispetto della certificazione e delle prescrizioni del GDPR, ma con la cooperazione di attori privati, ossia gli OdC. Nell'ottica del Regolamento, questi ultimi dovrebbero fungere da intermediari tra l'autorità di controllo e i soggetti regolati.

L'art. 43 GDPR, reca la disciplina relativa agli OdC, ribadendo, al primo paragrafo quanto detto dall'art. 42, ossia che: "*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. […]*". In questo modo, se con l'art. 42 il Legislatore europeo ha ideato un complesso compromesso tra autoregolamentazione e controllo, l'art. in commento rappresenterebbe lo strumento con cui questo delicato equilibrio co-regolativo si attua attraverso l'intervento di diversi attori[91]. In particolare, preminente è il ruolo degli OdC quali soggetti intermediari dei rapporti tra l'autorità pubblica, rappresentata dalle autorità nazionali di controllo competenti, e i soggetti privati che intendono certificarsi. Proprio per questo ruolo di crocevia, il GDPR prevede degli stringenti criteri affinché gli OdC possano essere qualificati (mediane la procedura di accreditamento) come tali, proprio in ragione del fatto che organismi saranno chiamati a valutare la *compliance* dei titolari e responsabili del trattamento ai fini dell'attribuzione della certificazione per la protezione dei dati personali.

4.1 Procedimento di accreditamento degli OdC: requisiti e condizioni

L'art. 43 GDPR dispone che gli Stati membri debbano garantire che gli OdC, affinché possano rilasciare o rinnovare le certificazioni, siano accreditati dall'autorità di controllo competente ai sensi degli artt. 55 e 56[92] ovvero dall'organismo nazionale di accreditamento designato in virtù del Regolamento (CE) n. 765/2008, conformemente alla norma EN-ISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo competente.

Tuttavia, né la norma in questione, né nel Regolamento si rinviene una vera e propria definizione del termine 'accreditamento'. Il significato di tale termine, piuttosto, può essere tratto dall'art. 2, n. 10 del Regolamento (CE) n. 765/2008, il quale definisce l'accreditamento come l'"*attestazione da parte di un organismo nazionale di accreditamento che certifica che un determinato organismo di valutazione della conformità soddisfa i criteri stabiliti da norme armonizzate e, ove appropriato, ogni altro requisito supplementare, compresi quelli definiti nei rilevanti programmi settoriali, per*

[91] Cfr. F. PEZZA, *Art. 43 – Organismi di certificazione*, in E. BELISARIO, G.M. RICCIO, G. SCOZZA (a cura di), *GDPR e Normativa Privacy*, Milano, 2020, 486.

[92] Precisamente l'art. 55 GDPR disciplina la competenza dell'autorità di controllo, stabilendo il principio per cui: "*Ogni autorità di controllo è competente a eseguire i compiti assegnati e a esercitare i poteri a essa conferiti a norma del presente regolamento nel territorio del rispettivo Stato membro*". Successivamente, l'art. 56 va a definire l'autorità di controllo capofila quale "*l'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare e del trattamento o responsabile del trattamento*" attribuendole il compito di agire in qualità di autorità di controllo capofila "*per i trattamenti transfrontalieri effettuati dal suddetto titolare del trattamento o responsabile del trattamento*".

svolgere una specifica attività di valutazione della conformità" [93] . Pertanto, l'accreditamento ai sensi dell'art. 43 GDPR dovrebbe essere inteso come l'attestazione autorevole, da parte di un organismo nazionale di accreditamento (o da parte di un'autorità di controllo nazionale), che un organismo di certificazione possiede le necessarie competenze e caratteristiche per svolgere l'attività di certificazione ai sensi degli art. 42 e 43 GDPR[94].

L'individuazione di tali requisiti, tuttavia, non è attività di poco momento, in quanto questi sono previsti dai vari paragrafi dell'articolato, intrecciandosi l'un l'altro e determinando un sistema coerente ma particolarmente complesso. Per dare chiarezza alle norme, la dottrina ha sottolineato che i requisiti sono suddivisibili in tre macrocategorie[95].

La prima categoria si riferirebbe alle qualità preesistenti di tali organismi, ossia la competenza, l'indipendenza e la terzietà rispetto ai soggetti da certificare. Per quanto concerne il requisito della competenza, l'OdC dovrà dimostrare specifiche abilità e conoscenze nell'ambito della protezione dei dati personali, acquisite, ad esempio, mediante la formazione specifica del personale dell'organismo o attraverso lo sviluppo di adeguata esperienza nello svolgimento di attività di *audit*[96].

La seconda classe concernerebbe i requisiti di tipo strutturale, vale a dire l'onere per gli OdC di predisporre procedure idonee per gestire dall'inizio alla fine il processo di certificazione in modo trasparente ed imparziale. L'OdC dovrà dimostrare all'accreditatore di aver previsto un sistema di efficace gestione delle funzioni ad esse assegnate, cioè delle procedure di rilascio, riesame periodico ed eventuale revoca delle certificazioni[97], nonché la predisposizione di un'effettiva struttura di monitoraggio[98].

Infine, la terza categoria concernerebbe un requisito di tipo operativo in base al quale gli OdC sono chiamati ad operare nel rispetto dei criteri di certificazione stabiliti e approvati ai sensi dell'art. 42, par. 5 dall'autorità nazionale di controllo competente o dall'EDPB. Questo perché l'attività dell'organismo di certificazione dipende in gran parte dall'ambito di applicazione e dal tipo di criteri di certificazione adottati, i quali ripercuoterebbero sulle procedure di certificazione. A fronte di ciò, l'esistenza di un

---

[93] Cfr. GPDP, *FAQ in materia di accreditamento e certificazione ai sensi del GDPR – parte generale*, in Rete: *https://www.garanteprivacy.it/regolamentoue/certificazione-e-accreditamento*, il quale precisa che: "*L'accreditamento è una forma indipendente e autorevole di attestazione della terzietà, competenza, imparzialità e adeguatezza degli organismi di valutazione della conformità (organismi di certificazione, ispezione e verifica e laboratori di prova e taratura)"*.

[94] Cfr. EDPB, *Linee guida 4/2018 relative all'accreditamento degli organismi di certificazione a norma dell'articolo 43 del regolamento generale sulla protezione dei dati*, 2019, 9, in Rete: *https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_it_0.pdf*.

[95] Cfr. F. PEZZA, *Art. 43 – Organismi di certificazione*, *op. cit.*, 489.

[96] Cfr. R. GIANNETTI, *La certificazione ai sensi del GDPR: standard per l'affidabilità del mercato data-driven*, in L. BOLOGNINI (a cura di), *Privacy e libero mercato digitale: convergenza tra regolazioni e tutele individuali nell'economia data-driven*, Milano, 2021, 218-220.

[97] Cfr. art. 43, par. 2, lett. c).

[98] In particolare, ai sensi dell'art. 43, par. 2, lett. d), gli OdC sono accreditati solo se "*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*".

meccanismo di certificazione e dei relativi criteri approvati è indispensabile affinché un OdC possa essere accreditato, determinando quindi la necessaria previa approvazione di un meccanismo di certificazione o la contestuale richiesta di convalida dei criteri alla richiesta di accreditamento.

Per quanto riguarda il procedimento di accreditamento, l'art. 43 si adopera per delineare le possibili opzioni percorribili. Come menzionato, gli Stati membri hanno l'obbligo di assicurarsi che gli OdC "siano accreditati" dall'autorità di controllo nazionale competente oppure dall'organismo nazionale di accreditamento individuato ai sensi del Regolamento (CE) n. 765/2008, conformemente alla norma EN-ISO/IEC 17065/2012. Per quanto riguarda la definizione dell'organismo nazionale di accreditamento, questi rappresenterebbe l'unico organismo che in uno Stato membro è stato autorizzato, da quest'ultimo, a svolgere l'attività di accreditamento, al fine di garantire uniformità di prassi nelle modalità di accreditamento[99].

A fronte di tale definizione, la particolarità del GDPR è che all'organismo nazionale di accreditamento viene affiancato l'autorità nazionale di controllo, come se l'importanza, o forse la specificità, della materia della *data protection* renda necessario anche l'intervento di quest'ultima autorità. Fermo tale elemento, il quale verrà analizzato più compiutamente *infra*, il Regolamento prevede un ulteriore condizione per l'accreditamento degli OdC da parte degli organismi nazionali di accreditamento, ossia che questo avvenga sulla base della norma tecnica EN-ISO/IEC 17065/2012, recante i requisiti degli OdC operanti limitatamente per la certificazione di prodotti, processi e servizi. Come precisato nel precedente capitolo, il preciso richiamo del GDPR alla EN-ISO/IEC 17065/2012, preclude la possibilità di considerare le certificazioni ISO/IEC 27001 e ISO/IEC 27701 conformi al GDPR, in quanto queste concernono la certificazione di un sistema di gestione, e non di prodotti, processi o servizi. Ciò determina l'impossibilità degli Organismi di Certificazione di sistemi di gestione per la sicurezza delle informazioni, accreditati secondo le norme ISO/IEC 17021-1 e ISO/IEC 27006, di essere accreditati anche per rilascio di meccanismi di certificazione prodotti ai sensi del GDPR, in quanto il substrato tecnico-normativo degli schemi di accreditamento è differente.

Per essere accreditati, quindi, gli OdC devono essere conformi alla EN-ISO/IEC 17065/2012. La norma tecnica in questione, tuttavia, per sua natura non presenta requisiti specifici per la protezione dei personali, prevedendo semplicemente l'accreditamento degli organismi nel processo di certificazione di prodotti. Inoltre, al fine dell'accreditamento sarà necessario uno schema di riferimento per poteri accreditare tramite la suddetta norma ISO. Il Regolamento, a tale riguardo, non fornisce indicazioni specifiche circa uno schema di certificazione di riferimento, facendo sostanzialmente rinvio ai meccanismi che saranno sviluppati nel corso del tempo dai privati. Pertanto, data l'assenza di specifici criteri, il Legislatore europeo ha dovuto prevedere come condizione ulteriore per l'accreditamento la soddisfazione di criteri autonomi predisposti da parte delle varie autorità nazionali competenti[100].

[99] Cfr. Art. 2, n. 11) Regolamento (CE) n. 765/2008: "*«organismo nazionale di accreditamento» l'unico organismo che in uno Stato membro è stato autorizzato da tale Stato a svolgere attività di accreditamento*".

[100] Cfr. L. BOLOGNINI, *Art. 43 – Organismi di certificazione*, in L. BOLOGNINI, E. PELINO, I. M. ALAGNA (a cura di), *Codice della Disciplina Privacy*, Milano, 2019, 297-299.

Pur apprezzando la finalità di specificare una norma tecnica apparentemente generica alla materia della protezione dei dati personali, non si può non evidenziare che affidare alla creazione delle varie autorità di controllo nazionali i criteri ulteriori per l'accreditamento potrebbe creare diverse incertezze normative date dalla possibile definizione di criteri differenti tra i vari Paesi membri. A fronte di tale circostanza, l'intervento dell'EDPB nell'approvazione dei suddetti requisiti aggiuntivi predisposti dalle autorità nazionali competenti è provvidenziale al fine di scongiurare l'eccessiva diversità e favorire quindi l'armonizzazione delle attività di accreditamento tra gli Stati membri[101]. Il Comitato, inoltre, si è pronunciato anche sulla possibilità di intervento delle autorità nazionali nell'attività di accreditamento direttamente da loro espletata. Favorire la produzione e la pubblicazione di criteri o linee guida, al fine di subordinare ad uno standard unico le attività di accreditamento degli OdC può essere utile sempre al fine di evitare un'eccessiva frammentazione dei criteri di accreditamento, soprattutto a fronte delle situazioni in cui si constati una violazione del Regolamento da parte degli OdC.

A fronte di queste iniziali considerazioni, il sistema di accreditamento non può che apparire inequivocabilmente complesso, in quanto è necessario definire i ruoli che gli OdC e l'autorità di controllo possiedono in merito. Definire la funzione che l'organismo di accreditamento può assumere all'interno di questo quadro risulta necessario e rilevante in quanto esso ha il potere di accreditare gli OdC in conformità dalla norma EN-ISO/IEC 17065/2012, specialmente, poi, se si considera l'intervento delle autorità di controllo. Accredia, per il caso italiano, così come gli altri organismi nazionali di accreditamento, infatti, non possono operare a meno che le rispettive autorità garanti nazionali non presentino i requisiti aggiuntivi e, nonostante attualmente in tutti i Paesi membri siano stati adottati i requisiti supplementari per l'accreditamento, tale situazione bloccante, sussistente nei primi anni di entrata in vigore del Regolamento, può aver contribuito a tardare lo sviluppo dei meccanismi di certificazione ai sensi del GDPR.

Relativamente al ruolo dell'autorità di controllo, il Comitato europeo per la protezione dei dati prende in considerazione l'art. 57, apr. 1, lett. q), il quale definisce che la procedura di accreditamento di un OdC viene effettuata dall'autorità di controllo, e l'art. 58, par. 3, lett. e) GDPR, che assegna alle autorità di controllo la facoltà di accreditare gli Organismi di Certificazione a norma dell'art. 43. Per quanto la formulazione di questi articoli avrebbe necessitato una maggiore chiarezza, si riscontra, nell'enunciato dell'art. 43, par. 1, flessibilità nella designazione delle funzioni di accreditamento. Difatti, tale compito non necessariamente dev'essere demandato solo all'autorità di controllo, ma può essere attribuito anche solo all'organismo nazionale di accreditamento o ad entrambi[102]. La mancata designazione dell'autorità garante,

[101] I requisiti previsti dall'art. 43, par. 1, lett. b) predisposti dai Garanti europei, infatti, devono essere necessariamente comunicati e approvati dal Comitato europeo ai sensi dell'art. 43, par. 6.

[102] Proprio la formulazione dell'art. 43, par. 1, garantisce che gli OdC possano essere accreditati da uno o da entrambi i soggetti richiamati: "*[…] 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*

tuttavia, non comporta il mancato coinvolgimento della stessa del procedimento di accreditamento; infatti, l'art. 43, par. 2, lett. a) impone all'OdC di dimostrare comunque all'autorità di controllo competente di essere indipendente e competente riguardo al contenuto della certificazione che intende conferire.

L'accreditamento dell'OdC ha un periodo massimo di cinque anni, rinnovabile solamente ove siano rispettate le condizioni previste dal Regolamento. Ciò, tuttavia, non toglie che l'autorità di controllo competente ovvero l'organismo nazionale di accreditamento possano revocare l'accreditamento quando, ai sensi dell'art. 43, par. 4-7, prima della scadenza naturale dell'accreditamento, vengano meno le condizioni per l'accreditamento stesso o quando queste non vegano più rispettate. Tale circostanza si verificherebbe ove le misure adottate da un OdC violino le prescrizioni del GDPR e, in particolare, quelle concernenti le condizioni di imparzialità rispetto ai terzi e adeguata competenza nella materia della protezione dei dati personali.

Infine, la disciplina sull'accreditamento può variare in ragione della possibilità dell'OdC di attribuire un Sigillo europeo per la protezione dei dati personali. La particolarità, in tal caso, è che una volta che i criteri del Sigillo sono approvati, ogni organismo di certificazione dell'unione può essere accreditato in ogni Paese membro per lo svolgimento dell'attività di certificazione. L'unico requisito posto per l'accreditamento concerne l'ambito territoriale di valenza dell'accreditamento. Come richiesto dalle Linee Guida 1/2018, l'accreditamento per l'applicazione del Sigillo dovrà avvenire nello Stato membro della sede principale dell'OdC che intenda utilizzare lo schema, "*ossia l'organismo responsabile del rilascio delle certificazioni e della gestione delle attività di certificazione delle proprie entità e affiliate in altri Stati membri. Laddove altri stabilimenti o uffici gestiscano ed effettuino certificazioni in autonomia, ciascuno di tali stabilimenti o uffici dovrà essere accreditato separatamente nello Stato membro in cui ha sede*". In altre parole, l'accreditamento per il Sigillo dovrà essere richiesto dall'OdC in ogni Stato membro in cui intenda operare quest'ultimo, mediante la propria sede principale e/o mediante altri stabilimenti[103].

4.2 Opzione dualistica o monistica per l'organismo nazionale di accreditamento

Come si è avuto modo di anticipare, il Regolamento consente a ciascuno Stato membro di determinare a chi spetti condurre le valutazioni necessarie all'accreditamento degli OdC, ossia all'autorità di controllo competente secondo gli artt. 55 o 56 GDPR, ovvero dall'organismo nazionale di accreditamento, sulla base della norma tecnica EN-ISO/IEC 17065/2012 e ai requisiti stabiliti dall'autorità garante competente, o da entrambi.

Gli Stati membri, quindi, potrebbero optare per un processo di accreditamento su base monistica, designando esclusivamente una delle autorità summenzionate, oppure affidare ad entrambe il compito di verificare gli OdC. Tuttavia, come riconosciuto dalla dottrina, l'esclusiva attribuzione all'autorità di controllo nazionale della competenza

EN-ISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo competente ai sensi degli articoli 55 o 56".

[103] Cfr. EDPB, *Linee Guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione*, *op. cit*., 16.

all'accreditamento degli OdC solleverebbe diversi dubbi in merito all'opportunità di tale decisione. Un primo quesito, infatti, riguarderebbe la natura discrezionale o meno di tale scelta: vale a dire se lo Stato membro sia libero di decidere secondo una valutazione assolutamente discrezionale se optare per l'alternatività o la cumulabilità degli enti preposti all'accreditamento, oppure se tale decisione debba tener conto di talune considerazioni di principio, e in particolare dei requisiti di indipendenza e terzietà di tutti i soggetti coinvolti nel processo di certificazione. Infatti, l'ente accreditatore dovrebbe essere terzo e indipendente dall'organismo di valutazione, quest'ultimo dovrebbe essere, a sua volta, terzo e indipendente rispetto dal soggetto da certificare e, infine, un'autorità garante, col compito di verificare il rispetto di queste condizioni da parte di tutti gli attori coinvolti, dovrebbe essere anch'essa soddisfare i medesimi requisiti di indipendenza e terzietà rispetto a tutti. È evidente che ove i compiti di accreditamento venissero attribuiti in via esclusiva all'autorità di controllo verrebbe a manifestarsi un paradosso in cui accreditatore, organismo di certificazione e autorità garante (fonte anche dei criteri integrativi di accreditamento), si concentrino in un'unica entità[104]. Per questo motivo, è da ritenersi che lo Stato membro, pur potendo attribuire discrezionalmente i poteri di accreditamento all'autorità che ritiene più opportuna, debba comunque bilanciare le attribuzioni delle varie entità coinvolte nel processo di certificazione, evitando di cadere nel sopraindicato paradosso.

Un ulteriore quesito, invece, concerne la valenza della norma tecnica EN-ISO/IEC 17065/2012 e dei parametri aggiuntivi *ex* art. 43, par. 1, lett. b) laddove l'accreditamento sia svolto dall'autorità di controllo. In questo caso, infatti, quest'ultima provvederà a stabilire la conformità dell'OdC ai requisiti previsti al paragrafo 2 dell'art. 43, però non è chiaro se a questi vadano associati anche i requisiti aggiuntivi richiamati. Dal paragrafo 3 del medesimo articolo, sembra trasparire il fatto che l'autorità di controllo debba tenere in considerazione anche requisiti aggiuntivi dalla stessa stabiliti in caso di accreditamento da parte dell'organismo nazionale di accreditamento[105], nulla dicendo, invece, in merito alla regolamentazione tecnica. A fronte di tale incertezza, volendo garantire coerenza tra le modalità di accreditamento e i requisiti dello stesso è da ritenere che le valutazioni dell'autorità di controllo dovrebbero comunque basarsi anche sulla regola ISO/IEC 17065, integrata ovviamene dai requisiti aggiuntivi stabiliti dalla stessa autorità[106].

In definitiva, lo Stato membro dovrà individuare una delle seguenti tre possibilità:

1. l'accreditamento è rimesso soltanto all'autorità di controllo nazionale. Tuttavia, rispetto ad alcune situazioni per cui è opportuno garantire la separazione delle

[104] Cfr. G.M. RICCIO, V. VITI, *Le "Certificazioni privacy" ed il Regolamento UE*, *op.cit*.

[105] Cfr. art. 43, par. 3, ove si evidenzia che l'accreditamento degli OdC ha luogo in base ai requisiti approvati dall'autorità di controllo competente o dal comitato e che i medesimi requisiti, laddove l'accreditamento sia svolto dall'organismo nazionale di accreditamento, integrano quelli previsti dal Regolamento (CE) n. 765/2008 e dalle norme tecniche.

[106] Cfr. EDPB, *Linee guida 4/2018*, *op.cit.*, 11. Questa soluzione è stata avvalorata anche dall'EDPB, il quale ha osservato che i requisiti previsti dall'art. 43, par. 2, rispecchiano e precisano i requisiti di cui alla norma ISO/IEC 17065.

funzioni di accreditamento e quelle di certificazione, o anche quella ispettiva, sarà necessario affidare un altro organismo terzo l'attività di accreditamento[107];

2. oppure è rimesso soltanto all'organismo nazionale di accreditamento, sulla base dei criteri *ex* art. 43, par.2 e a quelli fissati dall'autorità di controllo competente su integrazione dei requisiti e controlli della regola ISO/IEC 17065, e residuando, comunque, in capo a quest'ultima autorità i poteri di intervento per la revoca dell'accreditamento ai sensi dell'art. 43 par. 7;
3. oppure a entrambi i soggetti, sempre sulla base delle regole richiamate[108].

4.3 L'implementazione della disciplina GDPR sulle certificazioni all'interno degli Stati membri: l'esempio italiano

In Italia, l'art. 2-*septiesdecies*[109] d.lgs. 196/2003 ha recepito il disposto normativo dell'art. 42, par. 5 GDPR, designando quale autorità competente per l'accreditamento degli OdC l'ente unico nazionale di accreditamento istituito ai sensi del Regolamento (UE) 2008/765, ossia Accredia[110], subordinando l'intervento del Garante per la Privacy solamente in casi di gravi inadempimenti dell'ente.

Pertanto, di fronte alle opzioni riconosciute dal GDPR alla scelta degli Stati membri, l'ordinamento italiano ha optato per affidare ad entrambe le autorità il compito di accreditare gli OdC, pur preferendo Accredia quale soggetto cui competono in via regolare i suddetti poteri e permettendo l'intervento del GPDP solo in via di supplenza[111].

Con la delibera n. 148 del 29.07.2020 il Garante ha provveduto ad emanare il provvedimento relativo alla definizione dei 'requisiti aggiuntivi' di cui all'art. 43, par. 1, lett. b), che si andranno ad aggiungere a quelli previsti dalla norma tecnica ISO/IEC 17065:2012[112]. Il provvedimento, oltre a prevedere le condizioni ulteriori individuate dal

---

[107] Cfr. *ivi*, 12. In particolare, il Comitato prevede che "l*e autorità di controllo dovrebbero pertanto adottare misure organizzative atte a mantenere distinti i compiti che il regolamento generale sulla protezione dei dati individua, al fine di rendere solidi e facilitare i meccanismi di certificazione, evitando al tempo stesso possibili conflitti di interesse derivanti dall'esecuzione di tali compiti*". In tale ipotesi dovranno comunque essere considerati per la valutazione dell'accreditamento, sia i requisiti di cui all'art. 43, par. 2, sia le regole tecniche della ISO/IEC 17065:2012 e sia i criteri di accreditamento aggiuntivi.

[108] Rispetto a questa opzione rimane una certa incertezza rispetto all'inciso "*insieme tra loro*", perché non è chiaro se ciò alluda alla sussistenza di un potere di accreditamento disgiunto, in capo sia all'autorità di controllo nazionale che all'organismo nazionale di accreditamento, o alla necessità di un vero e proprio esercizio congiunto.

[109] Cfr. art. 2-*septiesdecies* d.lgs. 196/2003: "*L'organismo nazionale di accreditamento di cui all'articolo 43, paragrafo 1, lettera b), del Regolamento è l'Ente unico nazionale di accreditamento, istituito ai sensi del Regolamento (CE) n. 765/2008, del Parlamento europeo e del Consiglio, del 9 luglio 2008, fatto salvo il potere del Garante di assumere direttamente, con deliberazione pubblicata nella Gazzetta Ufficiale della Repubblica italiana e in caso di grave inadempimento dei suoi compiti da parte dell'Ente unico nazionale di accreditamento, l'esercizio di tali funzioni, anche con riferimento a una o più categorie di trattamenti*".

[110] Con decreto del MiSE del 22/12/2009, Accredia è stata costituita come associazione riconosciuta senza scopo di lucro che opera sotto la vigilanza diretta del MiSE (ora MIMIT).

[111] Cfr. L. BOLOGNINI, *Art. 43 – Organismi di certificazione*, *op.cit.*, 301-302.

[112] Cfr. GPDP, *Requisiti di accreditamento "aggiuntivi" dell'Autorità di controllo italiana con riguardo alla norma ISO/IEC 17065:2012 e in conformità dell'articolo 43, paragrafi 1, lettera b) e 3, del Regolamento*

Garante fornisce una serie di note esplicative, indicazioni pratiche ed esempi rivolti a facilitare l'applicazione dei requisiti introdotti.

Sulla base della struttura del provvedimento, è possibile differenziare i requisiti aggiuntivi in cinque macrocategorie:

1. Requisiti generali di accreditamento: in base al provvedimento l'OdC dev'essere in grado di dimostrare ad Accredia la conformità alle responsabilità giuridiche derivanti dall'accreditamento e, conseguentemente, dal ruolo che l'organismo andrà a ricoprire successivamente ad esso. In questi termini l'OdC, con la richiesta di accreditamento, si assumerebbe l'impegno di osservare ogni norma del Regolamento e del Codice Privacy applicabile allo svolgimento delle proprie funzioni, nonché di fornire prova dell'esistenza di procedure e misure rivolte al controllo e alla gestione dei dati personali, durante il processo di certificazione, dei soggetti richiedenti la certificazione [113] . Successivamente, vengono ampiamente descritte le condizioni dei c.d. 'accordi di certificazione', ossia del regolamento contrattuale che legherà il soggetto da certificare con l'OdC ai fini dello svolgimento delle procedure di verifica [114] . Ampio spazio, inoltre, viene fornito alla gestione dell'imparzialità e, in particolare, ai requisiti di indipendenza, imparzialità e di conseguente assenza di conflitto di interessi. In particolare, è previsto che l'OdC fornisca prova della propria indipendenza anche per quanto riguarda il finanziamento dell'organismo stesso, nella misura in cui tale aspetto possa incidere sulla sua imparzialità[115]. Il rischio principale, infatti, è quello per cui

---

Generale sulla Protezione dei Dati, r*egistro dei provvedimenti n. 148/2020,* 2020, in Rete: *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9445086*.

[113] Cfr. *ivi*, 2, nota 4.1.1 – Responsabilità giuridica. Sul punto, il Garante, nella nota esplicativa correlata, spiega che la prova dell'esistenza di tale requisito "*può essere costituita dalla designazione di un RPD ai sensi dell'articolo 37 del Regolamento e dall'adozione di politiche e procedure per la protezione dei dati (data protection policy) ai sensi dell'articolo 24, paragrafo 2 del Regolamento*".

[114] Cfr. *ivi,* 3. A fini puramente esaustivi, si riportano di seguito i principali requisiti che l'accordo di certificazione deve avere: 1) Deve imporre al soggetto da certificare (detto anche 'cliente') di ottemperare sempre sia ai requisiti generici di certificazione ai sensi della norma ISO/IEC 17065:2012, sia ai criteri approvati dal Garante o dal Comitato europeo per la protezione dei dati; 2) impongano al cliente di garantire nei confronti del Garante la piena trasparenza della procedura di certificazione; 3) non limitino la responsabilità del cliente in merito alla conformità al Regolamento, lasciando impregiudicati i compiti e i poteri del Garante; 4) impongano al cliente di fornire all'OdC tutte le informazioni e l'accesso alle attività di trattamento necessarie a espletare la procedura di certificazione; 5) impongano al cliente di rispettare tutte le scadenze e le procedure applicabili al procedimento di certificazione; 6) fissino regole sulla validità, sul rinnovo e sulla revoca della certificazione, inclusa la definizione di congrui intervalli di tempo per la rivalutazione o il riesame periodico in linea; 7) consentano all'OdC di divulgare al Garante tutte le informazioni necessarie al rilascio della certificazione; 8) contemplino regole in merito alle indagini sui reclami e sulla procedura di gestione degli stessi; 9) disciplinino tutte le conseguenze della revoca o della sospensione dell'accreditamento dell'OdC che si ripercuotono sul cliente; 10) impongano al cliente di informare senza indebito ritardo l'OdC e il Garante, su richiesta, in caso di modifiche significative della propria situazione di fatto o di diritto o dei propri prodotti, processi e servizi oggetto della certificazione.

[115] Cfr. *ivi*, 4-5. Sul punto, la nota esplicativa si riferisce all'OdC come "*una terza parte indipendente che non ha relazione con i soggetti che deve sottoporre a valutazione ai fini del rilascio della certificazione. La direzione (top management) e il personale dell'OdC responsabile della valutazione di conformità non devono aver ricoperto alcun ruolo nella progettazione, produzione, fornitura, […] del prodotto, processo o servizio oggetto di valutazione, né esserne i proprietari, gli utenti o i manutentori, e non possono agire in qualità di rappresentanti autorizzati di soggetti che abbiano ricoperto o ricoprano i suddetti ruoli*".

l'imparzialità dell'organismo sia compromessa ove questo sia finanziato o co-finanziato dai soggetti richiedenti le certificazioni o da associazioni di categoria particolarmente influenti. Infine, vengono svolte ulteriori considerazioni in tema di responsabilità e di riservatezza delle informazioni acquisite durante il rilascio delle certificazioni.

2. Requisiti relativi alle risorse umane: anche i requisiti concernenti la formazione e la competenza del personale dell'OdC sono particolarmente approfonditi. Nello specifico Accredia dovrà valutare che: il personale abbia competenze adeguate ed aggiornate riguardo alla protezione dei dati; sia indipendente e costantemente competente riguardo all'oggetto della certificazione, rispettandone i relativi criteri approvati; operi in assenza di conflitto di interessi; che il personale c.d. *decision maker* soddisfi determinati requisiti di onorabilità; abbia adeguate competenze ed esperienze rispetto alle misure tecnico ed organizzative di protezione dei dati, nonché conoscenze in materia informatica e giuridica. Le risorse umane dell'OdC, inoltre, dovranno essere adeguatamente aggiornate mediante formazione specifica del settore[116].
3. Requisiti di processo: i criteri individuati in questa categoria sono principalmente rivolti al processo di certificazione, riguardanti tutte le fasi della stessa. Sul punto, l'OdC, dovrà garantire: la chiara definizione dell'oggetto di valutazione della certificazione nella domanda di adesione; che siano sufficientemente descritti i metodi di valutazione necessari a determinare la conformità del/i trattamento/i ai criteri di certificazione e che questi siano standardizzati (al fine di garantire eguaglianza e terzietà rispetto ai soggetti da certificare, è previsto che ogni deroga ai mezzi di valutazione sia motivata dall'OdC). Inoltre, sempre in tema di valutazione, si specifica che l'OdC potrà avvalersi di *auditor* esterni e che si potranno tenere in considerazioni eventuali certificazioni preesistenti che coprano parte dell'oggetto della certificazione GDPR, facendo comunque salva ogni altra valutazione ritenuta necessaria [117]. In base al provvedimento, l'OdC, dovrà contemplare una procedura di riesame periodico, sorveglianza ed eventuale revoca delle certificazioni rilasciate al fine di verificare il mantenimento dei requisiti della certificazione. Infine, gli ulteriori requisiti concernono l'obbligo dell'organismo di tener conto di eventuali modifiche legislative, regolamentari, giurisdizionali o di prassi nell'ambito della protezione dei dati personali e che istituisca un meccanismo di reclamo attivabile, indistintamente, da un interessato,

---

Rispetto alla situazione di conflitto di interessi, questo per il Garante può sussistere quando: "*a) l'OdC abbia una qualsiasi relazione economica con il cliente tale da incidere sul proprio fatturato o generare anche parzialmente condizionamenti di natura economica; b) l'OdC, o i suoi soci, abbiano quote o partecipazioni in società che offrono consulenza rispetto a prodotti, processi, servizi oggetto di certificazione; c) l'OdC svolga attività assimilabili alla consulenza non adeguatamente mitigate, quali a esempio: […] la verifica dell'osservanza della normativa vigente, penetration test, intrusion detection*".

[116] Cfr. *ivi*, 8. In base alle note esplicative, "*si considera 'adeguato' il livello di competenza necessario all'effettivo svolgimento delle funzioni dell'OdC in relazione allo schema di certificazione per il quale viene richiesto l'accreditamento, avuto riguardo in particolare alle specificità del/i settore/i a cui si applica lo schema, alla categoria dei dati trattati e alla complessità delle attività di trattamento, ai diversi interessi coinvolti, nonché ai rischi per gli interessati*".

[117] Per approfondire v. *ivi*, 9-10.

ovvero da un organismo, organizzazione o associazione rappresentativa attiva nel settore della protezione dei dati personali.

4. Requisiti del sistema di gestione: con tali requisiti si ribadisce la necessità di documentare, valutare, controllare e monitorare in maniera indipendente l'attuazione, da parte dell'OdC accreditato, nell'ambito dell'applicazione del meccanismo di certificazione, di tutti i requisiti precedentemente richiamati. Dev'essere garantita la trasparenza [118] e la verificabilità dell'attuazione dei suddetti requisiti, nonché la permanente conformità agli stessi.
5. Ulteriori requisiti aggiuntivi: infine, in tale categoria, il requisito preminente è che l'OdC istituisca un sistema di aggiornamento dei metodi di valutazione secondo le modifiche del quadro giuridico e dello stato dell'arte, in modo di assestare le proprie modalità di valutazione ai nuovi rischi e vulnerabilità tecniche.

L'approvazione dei criteri del Garante della Privacy è stata oggetto di valutazione anche dall'EDPB. Come precedentemente illustrato, infatti, l'intervento del Comitato si rende necessario al fine di uniformare i criteri relativi all'attività di accreditamento, per evitare che queste attività divergano eccessivamente tra stato e stato, rendendo coerente l'applicazione del Regolamento. Proprio queste considerazioni sono state sollevate anche dal Comitato, con il Parere 23/2020[119], evidenziando come le proprie valutazioni sono rivolte ad analizzare principalmente gli scostamenti rispetto alle Linee Guida 4/2018, in quanto idonei a pregiudicare l'applicazione coerente del Regolamento[120]. Nel provvedimento in questione l'EDBP ha fornito alcuni suggerimenti rispetto a tutte le macrocategorie individuabili dal provvedimento n. 148/2020, esprimendo, in generale, come alcuni termini ed espressioni utilizzate dall'Autorità italiana non siano del tutto chiari. Proprio con riguardo ai requisiti per le risorse umane, l'EDPB ha raccomandato al GPDP di chiarire se il personale preposto alle valutazioni della certificazione debba essere iscritto ad appositi albi professionali ai sensi della normativa italiana, o meno. Inoltre, con riguardo ai requisiti di processo il Comitato ha sollevato come il Garante dovrebbe aggiungere che l'OdC, quando concede la certificazione, possa sollevare rilievi in merito a eventuali non conformità in un documento scritto. Ferme

[118] Cfr. *ivi*, 13-14. Proprio per garantire il requisito della trasparenza, il provvedimento prevede che l'OdC: "*a) tiene traccia dei principi alla base della valutazione di conformità; b) documenta le specifiche metodologie utilizzate nella definizione delle procedure di audit ai fini della valutazione di conformità; c) documenta le attività ispettive e di audit e i miglioramenti apportati alle procedure definite, comprese le motivazioni e la tempistica di tali miglioramenti; d) affida a soggetti terzi verifiche dei propri processi di valutazione della conformità; e) documenta e monitora il rispetto degli obblighi di imparzialità; f) motiva eventuali variazioni dei criteri di trasparenza documentale e di processo (in rapporto a singoli schemi di certificazione, alle modalità di verifica della conformità rispetto a tali schemi, ai requisiti minimi fissati nei contratti stipulati con i clienti)*".

[119] Cfr. EDPB, *Parere 23/2020 sul progetto di decisione dell'autorità di controllo competente dell'Italia relativa all'approvazione dei requisiti per l'accreditamento di un organismo di certificazione ai sensi dell'articolo 43, paragrafo 3 (RGPD)*, 2020, in Rete: *https://edpb.europa.eu/system/files/2022-11/edpb_opinion_202023_on_the_it_sa_accreditation_requirements_for_certification_body_it.pdf*.

[120] Nonostante ciò, l'EDPB ha giustamente riconosciuto come sebbene i requisiti per l'accreditamento siano sottoposti al meccanismo di coerenza, ciò non determina che questi debbano essere identici in quanto le autorità di controllo possono decidere discrezionalmente il contenuto degli stessi, facendo riferimento al proprio contesto e legislazione nazionale.

queste principali raccomandazioni, soprattutto per i requisiti delle risorse umane[121], le valutazioni dell'EDPB sono relativamente positive, avendo poi portato all'approvazione definitiva del provvedimento del Garante sui requisiti aggiuntivi.

In conclusione, come si è avuto modo di precisare, l'art. 2-*septiesdecies* mantiene in capo al Garante la facoltà di intervenire in materia di accreditamento, in caso di grave inadempimento di Accredia ai suoi compiti o con riferimento ad una o più categorie di trattamenti (per esempio, quelli a maggiore rischio), rispettivamente in via suppletiva o integrativa. La norma non disciplina le ipotesi di grave inadempimento o di intervento integrativo dell'autorità. Tuttavia, non è difficile immaginarsi che il Garante possa intervenire nel caso in cui Accredia violi le condizioni richieste dall'art. 43 GDPR, o dai requisiti aggiuntivi per il rilascio delle certificazioni, ovvero nell'eventualità in cui l'organismo nazionale di accreditamento risulti inadempiente rispetto ai propri obblighi di monitoraggio e controllo. In ogni caso, per una più efficace definizione di queste ipotesi, il Garante ha stipulato con la stessa Accredia un protocollo di intesa volto a favorire un più efficace scambio di informazioni e aggiornamenti relativamente alle attività di accreditamento ai sensi dell'art. 43 del Regolamento. Sulla base delle convenzioni stipulate[122], Accredia e il Garante dovranno scambiarsi vicendevolmente ogni eventuale informazione o documentazione ritenuta pertinente rispetto alle iniziative che entrambe assumeranno o intenderanno assumere sulla base delle informazioni l'un l'altro fornite. Attraverso questo meccanismo di cooperazione è facile ipotizzare che i casi di intervento 'autonomo' del Garante previsti dalle ipotesi di cui all'art. 2-*septiesdecies* saranno notevolmente ridotti.

5 Procedimento di certificazione, metodologia di verifica della conformità e monitoraggio successivo

Una volta definito il meccanismo di certificazione con i relativi criteri approvati dall'autorità di controllo competente, o dall'EDPB, ed essendoci un Organismo di certificazione accreditato a rilasciare quel determinato schema, titolari e responsabili del trattamento potranno vedersi attribuito il marchio o il sigillo della medesima. Quest'ultima avrà una durata massima di tre anni, rinnovabile alle stesse condizioni iniziali.

La breve durata della certificazione, insieme al termine di cinque anni per l'accreditamento degli OdC, dovrebbe assicurare, attraverso verifiche da ripetersi con cadenze prefissate l'aggiornamento del sistema d certificazione nel suo complesso e a garantire un suo costante monitoraggio.[123]

---

[121] Cfr. *ivi*, 8. Il Comitato ha ritenuto che solamente il requisito in merito alle risorse umane potesse comportare un'applicazione non coerente dell'accreditamento degli OdC.

[122] In particolare, la Convenzione dd. 20 marzo 2019 (in Rete: *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9099558*), poi rinnovata con la Convenzione dd. 20 marzo 2021 (in Rete: *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9570290*).

[123] Cfr. D. POLETTI, M.C. CAUSARANO, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione, op.cit.*, 399, nota 86.

Nella procedura di certificazione, il Regolamento prevede che gli OdC accreditati informino, prima della conclusione del procedimento di certificazione, l'autorità di controllo del rilascio o rinnovo di una certificazione[124]. Tale onere è rivolto a consentire all'autorità di esercitare i propri poteri ispettivi e correttivi di cui all'art. 58, par. 2, lett. h) GDPR, ossia di ingiungere all'OdC di non certificare il soggetto richiedente o di ritirare la certificazione, se i requisiti per la stessa non sono rispettati.

L'intervento dell'autorità garante dei dati personali nel processo certificativo si collega strettamente al regime di responsabilità degli Organismi di Certificazione. Questi, infatti, ai sensi dell'art. 43, par. 4, sono ritenuti responsabili della valutazione relative al rilascio della certificazione richiesta, fatta salva la specifica responsabilità del titolare o del responsabile del trattamento. In questo modo, le responsabilità e i ruoli dei certificatori e delle organizzazioni certificate verrebbero bilanciate secondo i rispettivi oneri e attribuzioni. Tale impostazione risulterebbe essere rivolta ad accertare la trasparenza, competenza e l'affidabilità degli OdC, i quali verrebbero valutati anche attraverso meccanismi indiretti di *feedback*, quali ad esempio azioni di responsabilità professionale, che progressivamente porterebbero ad espellere dal mercato i certificatori che non soddisfino i requisiti del Regolamento, o comunque meno professionali o rigorosi[125]. A ciò si aggiunge il fatto che gli organismi in questione sono sempre sotto il monitoraggio dell'autorità nazionale di controllo o dell'ente nazionale di accreditamento. Infatti, sulla base delle informazioni fornite prima del rilascio, nonché dopo ai sensi dell'art. 43, par. 5, l'autorità di controllo potrà assicurare l'effettiva applicazione dei requisiti e dei criteri di certificazione a norma del GDPR.

La comunicazione alle autorità di controllo delle certificazioni rilasciate dagli OdC dovrebbe essere funzionale anche per assicurare la trasparenza dell'intero contesto europeo della protezione dei dati personali. Infatti, i vari garanti europei dovranno, a loro volta, comunicare all'EDPB le informazioni sulle certificazioni rilasciate nei loro Stati membri, per permettere a quest'ultimo di raccogliere in un registro tutti i meccanismi di certificazione e renderli pubblici, con qualsiasi mezzo appropriato[126].

Con riferimento alla procedura di certificazione, e di accertamento della conformità del trattamento dell'organizzazione richiedente ai criteri di certificazione, l'EDPB con le Linee Guida 1/2018 esprime la necessità di adottare un modello metodologico proprio al fine di compiere le valutazioni inerenti al processo certificativo. Tale circostanza si somma all'onere di titolari o i responsabili del trattamento di fornire tutte le informazioni e l'accesso alle attività di trattamento necessarie a espletare la procedura di verifica dall'organismo di certificazione. Tale obblio rappresenterebbe un onere di collaborazione tra soggetto certificante e l'organizzazione del certificato rivolta ad incentivare la trasparenza nel compimento delle valutazioni per l'attribuzione delle certificazioni. Secondo questo modello si dovrebbe filosoficamente arrivare ad un punto

[124] Cfr. art. 43, par. 1.

[125] Cfr. D. POLETTI, M.C. CAUSARANO, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione, op.cit.*, 400.

[126] Cfr. Art. 42, par. 8. A tal fine, sul sito del Comitato è presente una pagina web dedicata alla pubblicazione dei meccanismi di certificazione, il quale, però, al momento è vuota: EDPB, *Register of certification mechanisms, seals and marks*, in Rete: *https://edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_en*.

per cui i soggetti che intraprendono il percorso certificativo forniscono loro stessi un apporto all'accertamento dell'ottemperanza alle regole a cui soggiacciono[127].

La garanzia della trasparenza, tuttavia, dev'essere assicurata non solo rispetto all'organizzazione del soggetto certificato e alla struttura del trattamento di dati personali, ma anche rispetto alla procedura di certificazione e, in particolare, nell'adozione da parte degli OdC di una precisa metodologia della valutazione. La trasparenza nel processo di certificazione può essere assicurata solo allorché gli organismi preposti alle valutazioni stabiliscano preventivamente quali informazioni raccogliere, come collezionarle e come documentarle.

Come rappresentato dall'EDPB ognuno di questi elementi metodologici si ripercuoterebbe ne valore e nella rilevanza della certificazione. Ad esempio, in tema di raccolta delle informazioni, adottare una procedura di raccolta su pura base documentale potrebbe essere insufficiente per verificare efficacemente la conformità ai criteri di certificazione; pertanto, una modalità di raccolta mediante accesso diretto o indiretto alla sede del titolare o responsabile del trattamento sarebbe ritenuta più congrua[128]. Inoltre, si evidenzia come le iniziative per il rilascio delle certificazioni dovrebbero comprendere misure specifiche rivolte a identificare quanto in profondità e con quale livello di dettaglio procedere alle valutazioni necessarie per soddisfare i criteri di certificazione. Infatti, la diversa scelta di profondità delle valutazioni si ripercuoterebbe sulla rilevanza e valore della certificazione, tale per cui una scarsa profondità si tradurrebbe in una minore rilevanza delle certificazioni, mentre un eccessivo dettaglio rischierebbe di limitare l'applicazione della certificazione[129].

Infine, sempre le Linee Guida precisano come la trasparenza del processo di certificazione debba essere assicurata mediante adeguata, accurata ed esauriente documentazione di quanto è stato certificato e della metodologia utilizzata. Gli OdC, quindi, dovranno formalizzare le motivazioni che hanno condotto a rilasciare e mantenere una certificazione e gli argomenti, il metodo di valutazione e le prove e

[127] Cfr. Art. 42, par. 6 GDPR; EDPB, *Linee Guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione*, *op. cit*., 20. Per esempio, il concetto di trasparenza potrebbe essere delineato come l'impegno del titolare o responsabile del trattamento di produrre documenti e rapporti che siano in grado di descrivere accuratamente i passi compiuti ed eventualmente i passi ancora da compiere all'interno di un'organizzazione per aderire ai criteri stabiliti per ottenere la certificazione.

[128] Cfr. EDPB, *Linee Guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione*, *op. cit*., 20. Al fine di garantire la rilevanza e l'efficacia della certificazione, il *Board* individua alcuni elementi metodologici che la procedura di valutazione deve contemplare, ossia: "*1) informazioni e indicazioni specifiche sui metodi di valutazione applicati e sulle risultanze raccolte, per esempio nell'ambito di controlli in loco o a partire dalla documentazione; 2) metodi di valutazione incentrati sui trattamenti (dati, sistemi, processi) e sulle finalità del trattamento; 3) l'identificazione delle categorie di dati, delle esigenze di protezione e dell'eventuale coinvolgimento di responsabili del trattamento o di terzi; 4) l'identificazione dei ruoli e l'esistenza di un meccanismo di controllo degli accessi che definisca ruoli e responsabilità*".

[129] Cfr. *ivi*, 21. Sul punto anche il comitato sottolinea chiaramente che "*Ai fini della dimostrazione della conformità, per mantenere la significatività potrebbe non essere sempre indispensabile raggiungere un livello molto dettagliato di analisi dei sistemi informatici utilizzati*", evidenziando come un eccessivo dettaglio nell'analisi potrebbe superare la capacità finanziaria del soggetto richiedente, limitando indelebilmente l'applicazione concreta delle certificazioni.

risultanti dell'applicazione dei criteri, oltre ai giudizi e alle interferenze raccolte durante il processo di certificazione[130].

Come detto, l'art. 42 par. 7 pone un termine massimo di validità delle certificazioni pari a tre anni. Essa può essere rinnovata, alle stesse condizioni, dall'ente che l'ha preliminarmente rilasciata quando continuino ad essere soddisfatti i requisiti stabiliti dai criteri di certificazione. Tuttavia, durante questa fase post-certificazione, i requisiti della stessa devono essere costantemente rispettati, potendosi determinare, in caso contrario, un'ipotesi di revoca della certificazione prima della sua naturale scadenza. La necessità di assicurare il persistente soddisfacimento dei requisiti della certificazione comporta che le organizzazioni certificate debbano essere monitorate. Proprio per tale necessità l'art. 43, par. 2, lett. c) prescrive che gli OdC, affinché possano essere accreditati, istituiscano un sistema di monitoraggio al fine di riesaminare periodicamente il rispetto dei requisiti di certificazione. Il Regolamento, nonché le varie linee guida, non prescrivono un determinato sistema di monitoraggio, lasciando ampia libertà agli OdC. Le possibilità spaziano dalla possibilità di istituire un meccanismo di osservazione continuo, tale per cui l'OdC possa effettuare, in qualsiasi e con ogni mezzo, un controllo affinché il trattamento certificato rispetti i criteri di certificazioni, ovvero un sistema di rinnovo-asseverazione periodico, in cui base al quale l'organizzazione certificata, per ogni determinato periodo (interno al termine massimo di validità) andrà a 'rinnovare' la certificazione attestando che non vi è stata alcuna modifica che incida in modo pregiudizievole sul rispetto dei requisiti della certificazione[131].

Come detto, nel caso in cui i requisiti della certificazione non siano rispettati durante il periodo di validità della stessa, questa potrà essere revocata da parte degli OdC oppure dell'autorità di controllo nazionale, o dal Comitato. In particolare, ove a disporre la revoca sia l'OdC, l'art. 43, par. 5 impone un dialogo con l'autorità di controllo competente alla quale deve trasmettere i motivi della revoca, nonché i motivi grazie ai quali la stessa certificazione è stata precedentemente rilasciata. In ogni caso, ove l'OdC rimanga inerte difronte agli inadempimenti del soggetto certificato, l'autorità nazionale di controllo, oltre a poter revocare direttamente la certificazione può anche ingiungere all'OdC di non rilasciare e/o rinnovare la certificazione laddove i requisiti per la certificazione non siano più soddisfatto, esercitando un potere di vigilanza sull'organismo stesso[132].

6 Ruolo e poteri delle autorità nazionali di controllo

Come evidenziato nell'introduzione del capitolo, la procedura di certificazione prevista dagli artt. 42-43 rappresenta una forma di co-regolamentazione. Ne consegue che, al centro del sistema di certificazione, le autorità pubbliche, rappresentate dalle autorità garanti, svolgono un ruolo significativo: sono queste ultime che devono

[130] Cfr. *ivi,* 21-22. Infine, viene anche precisato che "*Una documentazione dettagliata potrebbe essere il mezzo di comunicazione più indicato per consentire all'autorità di controllo di valutare se e in quale misura la certificazione possa essere riconosciuta nell'ambito di indagini formali*".

[131] In particolare, quest'ultimo modello è quello utilizzato nel meccanismo di certificazione canadese *Privacy by Design Certification*, sviluppato dalla Ryerson University e Deloitte Canada (vedi *infra* 158).

[132] Cfr. art. 43, par. 7; art. 57, par. 1, lett. o); art. 58, par. 1, lett. c) e par. 2, lett. h).

approvare i criteri per la definizione del meccanismo di certificazione e gli Stati membri sono lasciati liberi di rafforzare questi poteri, potendo riservare a queste autorità il ruolo di unici soggetti legittimati ad accreditare gli OdC.

Anche a fronte di tale esempio, è chiaro come il GDPR preveda una serie di modelli di regolazione delle certificazioni diversi, i quali coinvolgono differentemente l'autorità di controllo nazionale. Questa, infatti, può:

- rilasciare essa stessa la certificazione, nel rispetto del proprio schema autonomamente sviluppato;
- predisporre un proprio schema di certificazione e affidare la procedura di certificazione per il rilascio del sigillo agli Organismi di Certificazione;
- rilasciare essa stessa la certificazione, sulla base di schemi sviluppati da altri *scheme owner*;
- agire come Organismo di Accreditamento;
- assumere un mero ruolo di monitoraggio e di supporto per lo sviluppo di meccanismi di certificazione sul mercato[133].

L'autorità di controllo nazionale, tuttavia, non sarà libera di decidere quale ruolo svolgere, in quanto dovrà necessariamente tener conto delle decisioni legislative nazionali assunte in relazione alle modalità di accreditamento. Dato che il Legislatore può demandare all'autorità di controllo il ruolo di ente accreditatore degli OdC, si potrebbe sviluppare la situazione previamente evidenziata per cui *scheme owner*, OdC ed ente accreditatore coinciderebbero in un'unica entità, con possibile pregiudizio ai principi di trasparenza, indipendenza e terzietà che governano il sistema delle certificazioni nel GDPR.

Pertanto, se un'autorità di controllo decidesse di effettuare attività certificativa come un OdC, dovrà valutare attentamente il proprio ruolo in relazione ai compiti previsti dal Regolamento e dalla legislazione nazionale. Essa dovrà esercitare in modo trasparente le proprie funzioni, prestando particolare attenzione alla separazione dei poteri di indagine e di esecuzione, al fine di evitare ogni possibile conflitto di interessi.

Le Linee Guida 1/2018 evidenziano che, se l'autorità di controllo agisce in qualità di OdC, essa "*dovrà garantire l'adeguata istituzione di un meccanismo di certificazione e adottare criteri di certificazione o svilupparne di propri*". Dato che i procedimenti certificativi privati sono generalmente retti da contratti con le quali le parti si vincolano a seguire la procedura e i requisiti relativi ad essa, al fine del rilascio del sigillo o marchio, anche l'autorità di controllo come OdC dovrà stipulare con le singole organizzazioni richiedenti un accordo legalmente vincolante per l'erogazione dell'attività di certificazione. In assenza di atti legislativi o regolamentari, infatti, tale accordo è necessario per imporre i criteri di certificazione al soggetto richiedente e per espletare tutte le attività di valutazione, controllo, verifica e monitoraggio relative all'attività di certificazione[134].

Altrettanto problematico risulta la posizione dell'autorità di controllo nazionale ove decidesse di assumere il ruolo di *scheme owner*, sviluppando il proprio schema di certificazione. Questo in ragione del fatto che l'autorità di controllo, ai sensi dell'art. 42,

[133] Cfr. EDPB, *Linee Guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione*, *op. cit*., 10.
[134] Cfr. *ivi*, 11.

par. 5 GDPR deve approvare i criteri di certificazione proposti da uno *scheme owner* al fine dello sviluppo di una certificazione e, in questo caso, le figure si mescolerebbero, con il conseguente rischio di conflitto di interessi. Sul punto, il Regolamento nulla dice in merito alla possibilità dei Garanti europei di sviluppare direttamente meccanismi di certificazione, prevedendo, all'art. 42, par. 1, solamente che queste 'incoraggino' le attività dirette allo sviluppo di certificazioni. Proprio insistendo sul dato letterale della norma citata si potrebbe escludere la possibilità delle autorità di controllo di sviluppare autonomamente propri schemi di certificazione e limitando le loro attività ad un puro incoraggiamento del mercato[135]. Tuttavia, tale posizione sembra ormai superata dal fatto che la *Commission nationale pour la protection des données*[136] ha sviluppato e approvato un proprio meccanismo di certificazione applicabile nel territorio lussemburghese. Inoltre, rispetto al tema del possibile conflitto di interessi, vi è da dire che generalmente gli atti a contenuto significativo delle autorità di controllo europee ricevono, con parere, l'approvazione dell'EDPB, permettendo, mediante il meccanismo di cooperazione e coerenza di ricucire parzialmente il rapporto di autonomia tra *scheme owner*–autorità che approvi i criteri di certificazioni.

Gli altri ruoli che possono essere assunti dall'autorità di controllo nazionale non pongono particolari problematiche. Ove, infatti, non assumesse il ruolo di OdC ma solamente quello di *scheme owner*, sviluppando il proprio schema di certificazione, ma delegando l'attività di attribuzione della stessa ad un OdC differente, il principio di terzietà e di assenza di conflitti di interesse verrebbe regolarmente rispettato[137]. Medesime considerazioni si possono fare anche nelle ipotesi in cui l'autorità operi come ente di accreditamento, fermo restando le precitate criticità del ruolo rispetto agli organismi nazionali di accreditamento, o solo a monitoraggio delle attività svolte dagli altri organismi. In queste ultime due ipotesi, l'autorità si assicurerà di verificare il rispetto da parte di tutti gli organismi dei requisiti previsti dal Regolamento e, eventualmente, procederà a revocare le certificazioni o gli accreditamenti rilasciati o eserciterà i propri poteri di ingiunzione nei confronti degli Organismi di Certificazione.

Parallelamente alle autorità di controllo nazionale, anche l'EDPB ha diversi compiti operativi nel processo di certificazione. Il più impattante fra questi è il potere di intervento nella fase di elaborazione e approvazione dei criteri di certificazione ai sensi dell'art. 42, par. 5, con la conseguenza che, in questo caso, la certificazione avrà un campo applicativo esteso all'intero territorio dell'Unione, in quanto Sigillo europeo. Oltre a ciò, il Comitato riveste ulteriori ruoli: dev'essere informato circa i requisiti aggiuntivi di accreditamento dell'OdC[138]; raccoglie in un registro e rende pubblici "con qualsiasi mezzo appropriato" tutti i meccanismi di certificazione, al fine di garantire trasparenza al processo certificativo dei titolari e responsabile del trattamento; infine, ai sensi dell'art. 70, par. 1, lett. e)-n)-o)-p)-q), il Comitato può adottare linee guida,

[135] Cfr. EDPB, *Linee Guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione*, *op. cit*., 12. Anche l'EDPB è conforme a questa interpretazione, ricordando, inoltre, come "*Il regolamento generale sulla protezione dei dati attribuisce all'autorità di controllo il compito di approvare i criteri di certificazione, ma non di svilupparli*".

[136] L'autorità lussemburghese per la protezione dei dati personali (CNPD), in Rete: *https://cnpd.public.lu/en.html*.

[137] Cfr. L. BOLOGNINI, *Art. 42 – Certificazione*, in *Codice della disciplina privacy*, *op.cit.*, 296.

[138] Cfr. art. 43, par. 3.

raccomandazioni e migliori prassi per promuovere lo sviluppo e l'applicazione delle certificazioni, nonché per delineare con maggiore chiarezza i requisiti e le condizioni previsti dal GDPR. Al momento risultano tre le linee guida approvate aventi ad oggetto certificazioni ai sensi del GDPR:

1. Linee Guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione in conformità degli articoli 42 e 43 del Regolamento. Come visto nel paragrafo 3, l'obiettivo di tali linee guida è quello di precisare l'ambito di applicazione delle certificazioni e di stabilire i principi con cui individuare i criteri di certificazione. Le indicazioni dettate dalle Linee Guida 1/2018 sono state ulteriormente approfondite da un ulteriore A*ddendum* [139] . Con quest'ultimo documento vengono definite ulteriori raccomandazioni concrete destinate sia alle parti coinvolte nella redazione dei criteri di certificazione, sia alle autorità di controllo nazionale e all'EDPB stessa.
2. Linee Guida 3/2018 sull'accreditamento degli Organismi di Certificazione ai sensi dell'art. 43 del Regolamento generale sulla protezione dei dati. Scopo di queste linee guida è quello di armonizzare le prassi dei Paesi membri, delle autorità di regolamentazione e degli organismi nazionali di accreditamento per il procedimento di accreditamento ai sensi dell'art. 43.

Linee Guida 7/2022 sulla certificazione come strumento per i trasferimenti. Con questo documento l'EDPB fornisce indicazioni aggiuntive rispetto alle Linee Guida 1/2018 sui criteri di certificazione e stabilisce criteri ulteriori e specifici che dovrebbero essere inclusi in un meccanismo di certificazione da utilizzare come strumento per i trasferimenti verso Paesi terzi, alla luce delle garanzie individuate per altri strumenti di trasferimento ai sensi dell'art. 46 del GDPR (come le norme vincolanti d'impresa o i codici di condotta) e al fine di garantire un livello coerente di protezione, e tenendo conto della sentenza *Schrems II* (CGUE C-311/18).

7 Effetti e vantaggi della certificazione ai sensi del GDPR

Come precedentemente anticipato, l'adesione ad un meccanismo di certificazione è finalizzato a dimostrare l'effettiva predisposizione di quelle misure e garanzie richieste dal Regolamento in ragione del principio di *accountability*. Rispetto a tale considerazione, vi è da tener conto che la certificazione non è un mero strumento che attesti la conformità di un trattamento, ma è un mezzo che permette di ridurre i rischi derivanti dal trattamento stesso. In questi termini, la funzione 'probatoria' dello strumento certificativo è espressione del *risk based approach* assecondando la necessità di una corretta individuazione dei rischi ai diritti e libertà degli interessati.

L'idea sottostante agli artt. 42 e 43 GDPR, infatti, come d'altronde specificato dal considerando n. 100, è quella di poter dare agli interessati la possibilità di valutare in autonomia e rapidamente il livello di protezione dei dati personali nei servizi e prodotti

[139] Cfr. EDPB, *Guida alla valutazione dei criteri di certificazione – Addendum alle linee guida 1/2018 sulla certificazione e l'identificazione dei criteri di certificazione in conformità agli articoli 42 e 43 del Regolamento*, 2021, in Rete: *https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/Addendum%20Linee%20Guida%201_2018-DEF%20EN.pdf*.

che acquistano dal mercato. La funzione delle certificazioni, pertanto, non può essere ridotta ad una mera funzione probatoria, ma si articola, in realtà, in diversi effetti giuridici e vantaggi[140].

La certificazione è, in primo luogo, uno strumento di *trust & confidence*. Attraverso l'individuazione, da parte di un organismo terzo, dei criteri da rispettare per garantire la conformità del trattamento al Regolamento, la certificazione permetterebbe di ridurre la soggettività nella scelta dei mezzi di *compliance*. Per l'organizzazione del soggetto certificato, seguire degli standard univoci, nonché approvati dalle autorità preposte alla tutela dei dati personali, nella valutazione delle misure da implementare alla luce del principio di *accountability* genererebbe un sentimento di confidenza nella bontà delle misure tecniche ed organizzative adottate. Inoltre, tale senso di confidenza, nelle 'abilità' dell'organizzazione certificata, originerebbe effetti anche sul piano esterno, cioè verso gli interessati i cui dati sono trattati. Questi ultimi, per l'esattezza, riporrebbero maggiore fiducia nei confronti del trattamento svolto dal titolare o responsabile certificato, in quanto la certificazione evidenzierebbe in modo immediato che i trattamenti avvengono conformemente alla disciplina di riferimento[141].

Rispetto a questo binomio confidenza-fiducia si collegherebbero anche i vari effetti e vantaggi che deriverebbero dall'adesione ad una certificazione.

Il primo effetto è quello prettamente probatorio. Il Regolamento prevede che l'adozione di una certificazione costituisca una prova per dimostrare l'adeguatezza delle misure implementate per assicurare il rispetto del principio di *accountability*. La certificazione determinerebbe una presunzione di conformità delle misure adottate da titolare e responsabile del trattamento, in quanto il principio di *accountability* verrebbe attualizzato attraverso il procedimento di certificazione. L'organizzazione del titolare o responsabile, infatti, dimostrerebbe di aver percorso le varie tappe necessarie a mettere in atto le misure tecniche ed organizzative richieste dal Regolamento e, conseguentemente, dai criteri di certificazione per raggiungere quello *standard* adeguato di protezione dei dati personali necessario per superare la valutazione di conformità e conseguire il marchio o il sigillo. In questo modo, nonostante l'adesione ad un meccanismo di certificazione non riduca gli obblighi di *accountability,* si orienterebbero i destinatari del Regolamento ad una corretta costruzione della *privacy by design* e, in generale, della conformità al GDPR[142]. Infine, ritornando all'effetto dimostrativo della certificazione, questa comporterebbe una sorta di inversione dell'onere della prova nelle istruttorie compiute dall'autorità. Infatti, dato che l'organizzazione certificata avrà implementato tutte misure tecniche ed organizzative necessarie per assicurarsi la conformità ai criteri di certificazione, tutti i documenti e le evenienze probatorie eventualmente utilizzate nel processo certificativo potranno essere fornite all'autorità per dimostrare che l'adeguatezza delle misure stesse,

[140] Cfr. F. PEZZA, *Art. 42 – Certificazioni*, *op. cit.*, 479-480.

[141] Cfr. S. ZIEGLER, intervento presentato al seminario *Il meccanismo delle certificazioni con il GDPR – Il primo sigillo europeo per la protezione dei dati: la certificazione di Europrivacy*, *op. cit*.

[142] Cfr. S. SILEONI, *I codici di condotta e le funzioni di certificazione*, *op.cit.*, 934; G.M. RICCIO, V. VITI, *Le "Certificazioni privacy" ed il Regolamento UE*, *op.cit*.

dovendo poi quest'ultima autorità rinvenire ulteriori elementi istruttori per motivare l'inadeguatezza delle eventuali misure implementate[143].

Il secondo effetto, puramente giuridico, derivante dall'adesione ad un meccanismo di certificazione ai sensi del GDPR, concerne la possibile attenuazione del *quantum* delle sanzioni amministrative irrogate dall'autorità, ove si avveda di un'illegittimità nel trattamento. Come si è avuto modo di anticipare l'adesione ad una certificazione non riduce né gli oneri dei titolari e responsabili del trattamento, né la loro responsabilità, lasciando impregiudicato ogni potere ispettivo e sanzionatorio dell'autorità di controllo. Rispetto a tale situazione, tuttavia, la presenza di una certificazione dovrebbe esprimere la profonda competenza di un'organizzazione nel corretto e lecito trattamento di dati personali. È su questa premessa che l'art. 82, par. 2, lett. j) impone all'autorità di controllo di tener conto dell'adesione ad un meccanismo di certificazione al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa. L'inciso per cui l'autorità di controllo 'debba tener conto' della certificazione, tuttavia, non determina necessariamente un effetto attenuante nella determinazione del *quantum* dell'eventuale sanzione da irrogare, ma potrebbe costituire anche un'aggravante[144]. In ragione delle rilevanti competenze nella protezione dei dati personali attestate da una certificazione, infatti, il verificarsi di gravi violazioni del Regolamento potrebbe determinare l'aggravamento sanzionatorio, invece che l'attenuazione dello stesso. Ad esempio, se un titolare del trattamento certificato subisse un *data breach* e, in seguito all'attività ispettiva dell'autorità di controllo, quest'ultima si avveda che, in realtà, non erano state adottate, o comunque non sono state mantenute, quelle misure tecniche ed organizzative volte a mitigare il rischio della violazione dei dati personali, questa non potrà che irrogare un'elevata sanzione. Ciò avverrebbe in ragione del fatto che, il soggetto certificato che ha subito il *data breach*, avrebbe leso quell'affidamento che gli interessati riponevano nella certificazione. All'inverso, invece, se si ipotizzasse che la vittima certificata del *data breach* avesse rispettato quanto necessario per impedire il verificarsi di una violazione dei dati, è ragionevole presumere che l'autorità di controllo valuti positivamente la certificazione. Questa verrebbe considerata come un'attenuante nella determinazione del *quantum* della sanzione, dato che il titolare certificato aveva comunque implementato tutte le misure tecniche ed organizzative adeguate alla protezione dei dati personali[145].

Una considerazione simile può essere svolta anche sulla responsabilità del titolare del trattamento nella scelta del responsabile. In tal caso, il fatto di affidarsi ad un responsabile del trattamento certificato comporterebbe per il titolare del trattamento

[143] Cfr. L. BOLOGNINI, intervento presentato al seminario *Il meccanismo delle certificazioni con il GDPR – Il primo sigillo europeo per la protezione dei dati: la certificazione di Europrivacy*, *op. cit*.

[144] Cfr. EDPB, *Linee Guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione*, *op. cit*., 6.

[145] Considerazioni simili possono essere fatte anche in ambito prettamente giurisdizionale, nel quale le certificazioni potrebbero essere utilizzate per contestualizzare le norme di principio previste dal Regolamento, integrandone il contenuto con previsioni maggiormente puntuali, permettendo una maggiore certezza del diritto e prevedibilità degli esiti del giudizio. Rispetto a tale considerazione le certificazioni sarebbero assimilabili a delle fonti del diritto para-normative, quali fattori che potrebbero influenzare il giudice nella determinazione della *regula species* del caso concreto.

l'esclusione della responsabilità per *culpa in eligendo*, in quanto egli si sarebbe affidato ad un soggetto verso cui era legittimo presumere la competenza nell'ambito del trattamento di dati personali.

In terzo luogo, l'essere pronti a dimostrare la propria conformità può acquisire valenza competitiva e procurare vantaggi laddove alla certificazione si affianchi un meccanismo reputazionale. Come si è detto, ottenendo una certificazione si migliorerebbero le condizioni di trasparenza di un trattamento ottenendo un incremento della fiducia dei terzi e interessati rispetto alla conformità al GDPR dei prodotti o servizi a loro offerti [146] . L'aumento della fiducia nel trattamento determinerebbe ragionevolmente un effetto reputazionale sia all'interno dell'organizzazione del soggetto certificato, che all'esterno, verso gli altri *competitor.* Interno, in quanto le certificazioni possono essere usate per dar prova ai propri dipendenti e/o rappresentanze sindacali che il trattamento dei loro dati avviene con un alto grado di conformità; esterno perché le certificazioni potrebbero creare un'immagine pubblica positiva e garantire un vantaggio competitivo rispetto alle altre imprese sul mercato, attraendo nuovi clienti o partner[147]. In breve, il rispetto delle stesse determinerebbe, non solo la presumibile assenza di sanzioni giurisdizionali o amministrative, ma, soprattutto, una spinta del mercato, capace di valorizzare o sprofondare la reputazione di un'organizzazione in base alla presenza di una certificazione e dunque al rispetto o meno degli obblighi imposti dal GDPR[148].

Non solo; in futuro, la conformità della propria struttura organizzativa ai principi della *data protection* potrebbe essere necessario per soddisfare i requisiti di bandi per l'affidamento di servizi, appalti o lavori pubblici. Pertanto, le certificazioni ai sensi del GDPR risulteranno uno strumento quantomeno opportuno, se non necessario, per partecipare alle gare d'appalto pubbliche e, quindi, ci sarà un ulteriore ragione per dotarsi di questo tipo di strumento[149].

---

[146] Già il CNIL, l'autorità garante per la protezione dei dati francese, qualifica certificazioni e codici di condotta come '*confidence indicators*' (in Rete: *https://www.cnil.fr/en/privacy-seals*). Per approfondire l'applicazione delle certificazioni *data protection* nell'ordinamento francese v. J. CARVAIS-PALUT, *The French Privacy Seal Scheme: A Successful Test*, in R. RODRIGUES, V. PAPAKONSTANTINOU (a cura di), *Privacy and Data Protection Seals*, 2018, 49-58, in Rete: *https://link.springer.com/chapter/10.1007/978-94-6265-228-6_4*.

[147] Ad esempio, un titolare del trattamento sceglierebbe più facilmente un responsabile del trattamento certificato ai sensi del GDPR rispetto ad uno la cui conformità delle relative attività non è stata verificata.

[148] Cfr. S. SILEONI, *I codici di condotta e le funzioni di certificazione*, *op.cit.*, 933- 935. Sul punto, l'a. sottolinea come la violazione delle norme tecniche e criteri contenuti nelle certificazioni possa portare a risultati nefasti in termini di immagine e reputazione: spesso, infatti, le imprese più che essere preoccupare per sanzioni di natura amministrativa o azioni risarcitorie, sono attente alla possibilità che gli utenti (e quindi gli interessati) interrompano gli scambi dei propri dati, punendo così il titolare del trattamento inadempiente dei propri obblighi. Un esempio rispetto a quanto potrebbe accadere con riferimento alle certificazioni nei dati personali può essere colto dai modelli di certificazione ambientale: risulta chiaro, infatti, come le imprese siano spinte a aderire a certificazioni *green* poiché non vogliono essere identificate come soggetti che inquinino l'ambiente. Sul punto v. G. BACCELI, *Analisi economica del diritto dell'ambiente* e G. BELLOMO, *La gestione dell'ambiente ed i nuovi strumenti*, entrambi in G. DI PLINIO-P. FIMIANI (a cura di), *Principi di diritto ambientale*, Milano, 2008, 115-155.

[149] Cfr. T.A.R. Veneto Venezia, Sez. I, 04/01/2022, n. 8: "*In materia di appalto di fornitura di apparecchiature finalizzate alla rilevazione delle violazioni di cui all'art. 142 del D.Lgs. 30 aprile 1992, n. 285, poiché l'art. 345, comma 1, del D.P.R. 16 dicembre 1992, n. 495 statuisce che le apparecchiature destinate a controllare l'osservanza dei limiti di velocità devono essere costruite in modo da raggiungere*

Infine, certificati, sigilli e marchi, costituiscono, ai sensi degli artt. 42 e 46, par. 2 GDPR una delle soluzioni percorribili per il trasferimento di dati personali *extra* UE, purché accompagnate dall'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate. In prospettiva, le certificazioni potrebbero porsi quali alternative alle *standard contractual clauses* previste sempre dall'art. 46, par. 2, lett. c) per l'istituzione di garanzie adeguate, tenendo conto anche delle recenti critiche emerse in ordine all'efficacia di queste [150] . Sul punto, anche l'EDPB ha pubblicato ulteriori approfondimenti nelle Linee guida 7/2022 sulla certificazione come strumento per i trasferimenti in relazione all'utilizzo pratico delle certificazioni come strumento per i trasferimenti. Nel documento il Comitato sottolinea come le certificazioni debbano essere altamente *customizzate* alla luce delle attività oggetto di trattamento, dei dati trasferiti e della legislazione del paese terzo in cui i dati sono trasferiti. Vengono, inoltre, forniti criteri ulteriori e più specifici, rispetto alle valutazioni contenute nelle Linee Guida 1/2018, di cui tener conto nello sviluppo dei criteri di certificazione, fra cui:

- specifici criteri volti alla valutazione della legislazione del Paese terzo, richiedendo, ad esempio, all'importatore di documentare l'*assesment* del contesto legale e delle pratiche del paese in cui opera;
- obblighi generali di esportatori e importatori, prevedendo che accordi contrattuali (ad esempio in un contratto di servizi) tra esportatori e importatori descrivano il trasferimento specifico a cui si applica la certificazione e che i diritti dei terzi beneficiari sono riconosciuti agli interessati;
- meccanismi da attivare nei casi in cui la legislazione e le pratiche nazionali impediscano il rispetto degli impegni assunti nell'ambito della certificazione; e

detto scopo fissando la velocità del veicolo, in un dato momento, in modo chiaro ed accertabile, tutelando la riservatezza dell'utente e che le singole apparecchiature devono essere approvate dal Ministero dei lavori pubblici, ove l'apparato offerto dall'aggiudicataria risulti privo di omologazione relativamente ad alcune delle caratteristiche offerte e in ogni caso non utilizzabile in quanto comportante l'illecita registrazione dei dati di tutti i veicoli in transito, deve ritenersi che lo stesso non soddisfi i requisiti essenziali previsti dalla normativa di settore e non sia, quindi, compatibile con l'oggetto della prestazione dedotta nell'appalto", in *One Legale*.

[150] In particolare, ci si riferisce al provvedimento della *Data Protection Commission*, n. IN-20-8-1 del 12 maggio 2023, con il quale l'autorità garante dei dati personali irlandese ha sanzionato Meta Ireland per 1,2 miliardi di euro per illecito trasferimento di dati personali negli USA in assenza di garanzie adeguate, ingiungendole altresì di bloccare i trasferimenti di dati nel paese americano ove non si trovasse una soluzione tecnica o giuridica per assicurare garanzie adeguate. Sul punto v. DATA PROTECTION COMMISSION, *Data Protection Commission announces conclusion of inquiry into Meta Ireland*, 2023, in Rete: *https://www.dataprotection.ie/en/news-media/press-releases/Data-Protection-Commission-announces-conclusion-of-inquiry-into-Meta-Ireland* (per il provvedimento: *https://edpb.europa.eu/system/files/2023-05/final_for_issue_ov_transfers_decision_12-05-23.pdf*);
EDPB, *Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR)*, 2023, in Rete: *https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-12023-dispute-submitted_en*; A. LONGO, *Meta, sanzione privacy 1,2 miliardi e rischio blocco di Facebook in Europa*, in *Cyber Security 360*, 2023, in Rete: *https://www.cybersecurity360.it/legal/privacy-dati-personali/meta-sanzione-privacy-miliardaria-e-rischio-blocco-in-europa/*.

- misure per la gestione di richieste di accesso ai dati da parte delle autorità del Paese terzo[151].

[151] Cfr. EDPB, *Linee guida 7/2022 sulla certificazione come strumento per i trasferimenti*, 2023, in Rete: *https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_07-2022_on_certification_as_a_ tool_ for_transfers_v2_it_0.pdf*.

CAPITOLO III - GLI ATTUALI SCHEMI DI CERTIFICAZIONE IDONEI AI SENSI DEL GDPR

1 Lo Studio Tilburg per l'identificazione degli schemi di certificazione idonei ai sensi del GDPR

Gli anni precedenti all'entrata in vigore del GDPR sono stati caratterizzati da diverse riflessioni in relazione alle certificazioni per la protezione dei dati personali. Infatti, il panorama tecnico già comprendeva svariati schemi sul tema della *data protection* e *cybersecurity*, i quali, tuttavia, risultavano inadeguati rispetto alle prescrizioni indicate dal nuovo Regolamento.

Le certificazioni ISO/IEC 27001 e ISO/IEC 27701 rappresentano l'esempio più lampante di tale diversità, in quanto non formate sullo standard ISO/IEC 17065 attestante prodotti, processi e servizi. Le citate norme tecniche, tuttavia, non figurano le uniche esperienze di certificazioni anteriori all'entrata in vigore del Regolamento. Diverse iniziative, infatti, erano state condotte in Germania, e in particolare nel *Land* Schleswig-Holstein. La normativa sul trattamento dei dati personali del *Land* prevedeva che gli organismi pubblici, nelle gare per l'affidamento di forniture e approvvigionamenti, dovessero accordare preferenza a prodotti e servizi informatici certificati con un marchio rilasciato dall'Autorità per il trattamento dei dati personali del Schleswig-Holstein (ULD)[1]. Questo sistema costituirà poi la base per la creazione della certificazione EuroPriSe, sviluppato dalla stessa ULD in cooperazione con il CNIL[2] e AEPD[3], di cui si dirà di seguito[4]. In Francia, inoltre, con la riforma del 2004 della legge in materia di protezione dei dati personali, era prevista la possibilità della CNIL di rilasciare un sigillo per prodotti o procedimenti finalizzati alla protezione delle persone fisiche con riferimento ai loro dati personali. In tal caso i criteri di certificazione e il ToE, su cui approfondire la conformità, vengono identificati direttamente dal CNIL sulla base della legge francese[5].

Con l'entrata in vigore del GDPR, tuttavia, e il mancato approfondimento dei temi relativi alle certificazioni, si creò un contesto di scarsa chiarezza rispetto alle certificazioni conformi al Regolamento. Tale situazione, avrebbe potuto creare diversi problemi in tema di trasparenza, soprattutto rispetto all'eventuale esibizione di documentazione adeguata che attestasse la conformità al GDPR.

---

[1] In Germania, esistono diverse autorità di protezione dei dati personali rispettivamente per ogni *Land.* A livello federale, poi, è stata istituita la BfDI (The Federal Commissioner for Data Protection and Freedom of Information. Per approfondire v. B. CUSTERS, F. DECHESNE, A. M. SEARS, T. TANI, S. VAN DER HOF, *A comparison of data protection legislation and policies across the EU*, in Computer Law & Security Review, 2018, vol. 34, 234-243, in Rete: *https://doi.org/10.1016/j.clsr.2017.09.001*.

[2] Ossia l'Autorità di controllo dei dati personali francese, la *Commission nationale de l'informatique et des libertés*, in Rete: *https://www.cnil.fr/fr/les-missions-de-la-cnil*.

[3] Ossia l'Autorità di controllo dei dati personali spagnola, la *Agencia española protección datos*, in Rete: *https://www.aepd.es*.

[4] Cfr. A.R. POPOLI, *Codici di condotta e certificazioni*, *op.cit*. 409.

[5] Cfr. D. POLETTI, M.C. CAUSARANO, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, *op.cit.*, 405-406.

Per tali motivi nel febbraio 2019 l'Università di Tilburg [6], su iniziativa della Commissione europea, ha concluso uno studio sui meccanismi di certificazione per la protezione dei dati personali per valutare la situazione generale sul tema e individuare i potenziali schemi di certificazione conformi agli artt. 42 e 43 del Regolamento. Lo studio ha evidenziato come nel mondo fossero disponibili 117 schemi di certificazione che prendevano a riferimento la privacy, di cui 97 con origine in Europa. Di questi, solo 15 sono entrati nella *shortlist* dello studio, come *best practices* per la protezione dei dati personali, venendo ognuna approfondita al fine di verificarne la conformità al GDPR. La ricerca non è stata limitata solamente alle certificazioni presenti negli Stati membri dell'UE, ma anche rispetto a paesi *extra*-UE in quanto, data la novità dell'introduzione degli artt. 42 e 43 si è ritenuto necessario analizzare tutti i possibili schemi di certificazione già operativi nel mercato che potessero essere attinenti alla protezione dei dati personali e alla privacy. Anche le se certificazioni *extra*-UE non rientravano nel campo applicativo dei menzionati articoli, acquisire la loro 'esperienza' e operatività pareva poter arricchire lo sviluppo delle certificazioni conformi al GDPR.

Sulla base di questa lista, poi, i ricercatori hanno selezionato, sulla base di una serie di criteri specifici e dopo una consultazione con la Commissione europea, le 15 certificazioni da analizzare specificatamente per verificarne la rispondenza al Regolamento[7]. I criteri messi in campo per la selezione delle certificazioni sono stati: il rispetto dei requisiti fondamentali derivanti dagli artt. 42-43 GDPR[8]; la previa operatività dello schema; l'oggetto o la tematica oggetto di valutazione con la certificazione[9]; la portata territoriale della normativa su cui si basa la certificazione[10]; i soggetti interessati (ossia titolari o responsabili del trattamento o entrambi); la natura settoriale o 'neutra' della certificazione[11].

---

[6] Cfr. EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, G. BODEA, K. STUURMAN, M. BREWCZYŃSKA, *Data protection certification mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679: final report*, 2019, in Rete: *https://data.europa.eu/doi/10.2838/115106*.

[7] Cfr. *ivi*, 32. La problematica principale dello studio è stato il reperimento delle informazioni. Per realizzare la lista estesa delle 117 certificazioni, infatti, "*the research team used a literature review of previous studies relevant to data protection certification, scientific articles published in the field, Internet search and other communications means*". Inoltre, organizzare le informazioni raccolte per poi compararle risultava difficile in quanto i diversi meccanismi di certificazione usavano termini e linguaggi differenti.

[8] Cfr. *ivi,* 35. La logica della ricerca, infatti, è che gli schemi di certificazione che saranno sottoposti a studio approfondito siano pertinenti all'ambito di applicazione dell'art. 42 GDPR. Tali criteri, quindi, fungeranno da linee guida per selezionare primariamente le certificazioni da approfondire o meno. In particolare, queste ultime: 1) dovranno concernere dati personali o privacy in senso lato; 2) dovranno essere volontarie; 3) dovranno essere attribuite solo da un organismo terzo (e non auto-certificazioni); 4) dovranno concernere operazioni di trattamento.

[9] Cfr. *ivi,* 36. In particolare, tenendo conto del fatto che le certificazioni possono essere limitate ad un argomento preciso oppure essere generiche, si è valutato se la certificazione fosse: comprensiva, concernendo, in generale il trattamento di dati personali, oppure relativa alla DPbDD, alla sicurezza dei dati o al trasferimento/comunicazione.

[10] Cfr. *ibidem*. Lo studio, avendo ad oggetto certificazioni presenti sia nelle giurisdizioni dei paesi membri dell'UE sia giurisdizioni di stati terzi, ha tenuto conto sia delle certificazioni basate sulla regolamentazione comunitaria, sia di quelle basate sulla legislazione, nazionale o regionale, di paesi non UE.

[11] Cfr. *ibidem*. Questo criterio, in particolare, mira a prestare attenzione alle certificazioni relative a settori specifici. Infatti, anche se il GDPR è un regolamento generale, gli adempimenti dei titolari e responsabili

Sulla base di questi criteri, le 15 certificazioni che sono state selezionate per essere analizzate: "*1. BS 10012 Personal Information Management System Certification (UK); 2. TÜV Italia ISO/IEC 27001 Information Security Management Certification; 3. BSI ISO/IEC 27018 Information technology. Security techniques. Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors Certification (UK); 4. Certificazione ISDP©10003:2015 Data protection (IT); 5. Datenschutzaudit beim ULD (DE); 6. E-privacy app (DE); 7. EuroPrise - the European Privacy Seal (DE); 8. IkeepSafe Coppa Safe Harbor (US); 9. Label CNIL digital safe boxes (FR); 10. Health Personal Data Storage Agreement (FR); 11. Myobi Privacy Seal (NL); 12. Norea Privacy-Audit-Proof (NL); 13. PrivacyMark System (JP); 14. Privacy by Design Certification Ryerson (CA); 15. TrustArc APEC CBPR certification (US)*"

Di questi, solo due certificazioni sono risultate in linea al GDPR: lo schema italiano ISDP©10003 e il menzionato schema tedesco EuroPriSe. La selezione compiuta dai ricercatori di Tilburg ha avuto ad oggetto diversi parametri, fra cui lo scopo, i criteri di certificazione, le modalità di verifica della conformità, le modalità di rinnovo, il sistema di monitoraggio, le *policy* per la violazione della certificazione e le modalità di risoluzione dei reclami. Particolare attenzione, poi è stata posta in relazione alla flessibilità degli schemi rispetto ai diversi settori e ai processi merceologici[12]. Chiaramente, dato che si intendeva analizzare le possibili certificazioni rilevanti ai sensi del GDPR, si è posta particolare attenzione alla struttura del sistema di certificazione e alla sua rispondenza ai principi disposti dagli artt. 42 e 43. È a tale ragione che si deve lo scarso numero di certificazioni considerate rientranti nello scopo del GDPR. Infatti, la grande maggioranza degli schemi non rispondeva alla norma ISO/IEC 17065 per la certificazione di prodotti e servizi richiamata dall'art. 43 GDPR, basandosi, invece, sulla ISO/IEC 17021-1, relativa ai requisiti per gli Organismi di Certificazione che svolgono *audit* e certificazioni di sistemi di gestione[13]. Un ulteriore criticità riscontrata nello studio è il mancato aggiornamento degli schemi sviluppati in Europa alle norme del Regolamento, nonché il ridotto ambito applicativo territoriale, in quanto limitato ai singoli stati membri. Infine, rispetto agli schemi *extra*-europei lo studio ha evidenziato come questi ultimi siano inapplicabili nei paesi dell'UE, in ragione delle notevoli differenze sulla disciplina della protezione dei dati personali[14].

Nonostante le poche certificazioni rientranti nello scopo del GDPR, lo studio ha comunque tratto dei preziosi insegnamenti. Le certificazioni già esistenti, infatti, dispongono già di metodologie di valutazione, schemi contrattuali per la gestione dei

del trattamento sono suscettibili di differire considerevolmente in relazione al diverso settore in cui operano.

[12] Cfr. *ivi,* 46-57.

[13] Cfr. R. GIANNETTI, *La certificazione ai sensi del GDPR: standard per l'affidabilità del mercato data-driven*, *op. cit.*, 227-228.

[14] Cfr. EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, G. BODEA, K. STUURMAN, M. BREWCZYŃSKA, *Data protection certification mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679: annexes*, 2019, 66-72, in Rete: *https://data.europa.eu/doi/10.2838/297807*. Spiccano, fra i vari schemi, le valutazioni rivolte allo schema canadese *Privacy by Design Certification*, in quanto, anche se il Canada ha una normativa e cultura *data protection* più profonda, la certificazione presa in considerazione non rientrerebbe tra quelle relative al GDPR in quanto certifica sistemi di gestione. Inoltre, viene sollevata la questione rispetto all'accreditamento di OdC non europei per la possibile 'valenza' della certificazione nell'UE.

rapporti tra OdC e soggetto richiedente e di strutture organizzative composte da *auditors* esterni che possono essere utilizzati anche nella creazione di meccanismi di certificazione conformi al GDPR. Proprio verso gli *auditors* può essere tratta un ulteriore lezione: se l'OdC, e il suo personale interno, non possiede quelle capacità e competenze necessarie per verificare la conformità di organizzazioni terze ai criteri di certificazione (e quindi al GDPR), la migliore soluzione è quella di collaborare con personale esterno, il quale si occuperà di svolgere le verificazioni tecniche necessarie per l'attribuzione del marchio di certificazione[15].

Infine, si è rilevato come sia i modelli di certificazioni generici (c.d. *one-size-fits all*), sia quelli dedicati a trattamenti particolari o specifici/personalizzati, sono compatibili con il GDPR. Tuttavia, il grado di trasparenza dello scopo della certificazione e la validità della metodologia di valutazione saranno questioni fondamentali per determinare se la certificazione rientri o meno nell'alveo di quelle rilevanti ai sensi del Regolamento[16]. Infatti, senza una piena trasparenza, le certificazioni sarebbero inutili e produrrebbero un effetto contrario rispetto a quello perseguito dal GDPR, ossia l'aumento della sfiducia nei trattamenti di dati personali e nelle nuove tecnologie. In questo modo, una maggiore trasparenza nello sviluppo e diffusione di meccanismi di certificazione conformi al GDPR può eliminare l'asimmetria informativa presente tra gli interessati e i titolari o responsabili del trattamento, permettendo, di conseguenza, una migliore circolazione dei dati personali.

2 Lo schema ISDP©10003:2020 per la protezione dei dati personali

Le organizzazioni che intendono certificarsi ai sensi del GDPR possono fare riferimento alla ISDP©10003:2020 "Schema internazionale per la valutazione della conformità al Regolamento europeo 2016/679" accreditato da Accredia secondo la norma UNI EN ISO 17065 e sviluppata dallo *scheme owner* Inveo[17]. La rispondenza di questo schema al GDPR è data dal fatto che questo si fondi sulla ISO/IEC 17065, come richiesto dall'art. 43 del Regolamento.

Proprio lo studio Tilburg ha positivamente evidenziato come la ISDP©10003, rientrando nel campo di applicazione degli artt. 42 e 43 GDPR, permette di coprire tutte gli aspetti della *compliance* richiesti dal Regolamento con un unico schema, determinando minore complessità, e soprattutto inferiori costi, per le PMI che intendono certificarsi[18].

---

[15] Cfr. EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, G. BODEA, K. STUURMAN, M. BREWCZYŃSKA, *Data protection certification mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679: final report*, *op.cit.*, 58-59.

[16] Cfr. *ibidem*.

[17] Al fine di garantire la trasparenza, i criteri di certificazione sono stati pubblicati sul sito web dello *scheme owner*. Tale scelta è determinata dalla volontà di Inveo di diffondere la cultura della *data protection*; fornire delle linee guide per un adattamento del titolare e del responsabile al GDPR; creare i presupposti per una certificazione conforme al Regolamento. Disponibile in Rete: *https://www.inveo.com/certificazione-isdp-10003-2020-data-protection*.

[18] Cfr. EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, G. BODEA, K. STUURMAN, M. BREWCZYŃSKA, *Data protection certification mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679: annexes*, *op. cit.*, 53-57.

Scopo della ISDP©10003:2020 è fornire i principi e gli elementi di controllo ai titolari e responsabili del trattamento, anche fuori dall'Unione europea, per dimostrare, ai sensi dell'art. 42, la conformità al GDPR dei trattamenti di dati personali effettuati nell'ambito dei prodotti, processi e servizi realizzati. In questo modo, l'organizzazione certificata garantirebbe fiducia alle terze parti che interagiscano con la stessa e permetterebbe di sviluppare procedure sicure, documentate e standardizzate da poter 'opporre' all'autorità di controllo per l'implementazione di misure adeguate[19].

L'oggetto della certificazione è quello di verificare la corretta attuazione del principio di *accountability*, dettagliando i requisiti e i controlli necessari, affinché i dati personali siano trattati secondo criteri di esattezza, accuratezza, attualità, coerenza, completezza e aggiornamento, richiesti dalla normativa vigente sulla protezione dei dati personali. Per tale ragione l'ambito di applicazione della certificazione è di carattere generico e non limitato ad un settore specifico. Lo schema può essere applicato ad ogni trattamento, o all'insieme di trattamenti, di dati personali coinvolti in un prodotto o servizio, a procedure, a processi di *governance* e all'eventuale rapporto intercorrente tra il titolare e il responsabile del trattamento, indipendentemente dalla tipologia, dimensione e natura dei prodotti, processi e servizi forniti[20]. La scalabilità della certificazione garantisce, quindi, la possibilità di limitare il piano di verifica del trattamento a quei controlli idonei e rilevanti rispetto al contesto del processo o servizio.

Come menzionato, la ISDP©10003 è applicabile sia ai titolari del trattamento, per la dimostrazione del livello di protezione dei dati ai sensi degli artt. 24 e 25 GDPR, sia ai responsabili esterni, per la dimostrazione delle garanzie sufficienti che devono presentare per il trattamento. Inoltre, i medesimi requisiti possono essere adottati dai titolari o responsabili del trattamento *extra*-UE, per sviluppare le misure e le competenze adeguate a trattare i dati personali europei importati ad un livello tendenzialmente adeguato[21].

Per quanto riguarda la struttura, lo schema ISDP©10003 prevede inizialmente una serie di requisiti generali attinenti al GDPR, a cui il titolare e il responsabile del trattamento devono conformarsi per raggiungere lo scopo della certificazione, e specifica l'approccio metodologico delle valutazioni[22]. Lo schema di valutazione della certificazione, infatti, adotta un approccio per processi, ossia che va a considerare l'insieme dei trattamenti di dati personali svolti, degli strumenti *software* e *hardware* utilizzati nell'organizzazione e le politiche che regolano l'operatività dei diversi trattamenti. Il titolare e/o il responsabile, quindi, dovranno verificare che ogni unità operativa coinvolta nel trattamento dei dati sia conforme ai criteri di *audit* e al

[19] Cfr. INVEO, *Certificazione ISDP©10003 per la valutazione di conformità al GDPR*, 2020, in Rete: *https://www.in-veo.com/certificazione-isdp-10003-2020-data-protection*.

[20] Cfr. INVEO, *ISDP©10003, Schema internazionale per la valutazione della conformità al Regolamento Europeo 2016/679*, 2020, 6, par. 1.2, in Rete: *https://www.in-veo.com/privacy-tools-new/schema-di-certificazione-isdp-c-10003-dw/37-schema-di-certificazione-isdp-10003-2020-rev-01-ita-new-release*.

[21] Si ricorda, infatti, che la certificazione non è ancora stata approvata ai sensi dell'art. 42, par. 5 GDPR.

[22] In particolare, vengono ribadite le definizioni dei principi di: adeguatezza delle misure organizzative; liceità correttezza e trasparenza; chiarezza e limitatezza delle finalità del trattamento; pertinenza dei dati trattati; minimizzazione dei dati trattati; qualità ed esattezza dei dati; limitazione della conservazione; sviluppo di una DPIA per la valutazione dei rischi del trattamento; adozione delle misure di sicurezza adeguate e comunicazione delle violazioni.

Regolamento, in modo che questi possano poi essere riesaminati ed eventualmente corretti, se necessario, dall'OdC.

In base allo schema, i processi che permetterebbero di monitorare il rispetto dei principi fondamentali richiamati dal Regolamento, sarebbero sette: 1. Politiche e obbligazioni del titolare; 2. Soggetti coinvolti nel processo del trattamento; 3. Principi applicabili al trattamento e tutela dei diritti; 4. Processi di adeguamento in fase di ideazione ed all'atto del trattamento a norma dell'art. 25; 5. Obblighi generali, gestione del rischio e sicurezza dei trattamenti; 6. Valutazione d'impatto; 7. Trasferimento dei dati personali verso paesi terzi, IoT, e *cloud computing*[23].

Successivamente viene ribadito che l'organizzazione che si sottopone alla certificazione ISDP©10003 deve, nella misura necessaria e nei limiti dei trattamenti dei dati effettuati, predisporre e mantenere aggiornata la documentazione GDPR obbligatoria e necessaria alla dimostrazione della *compliance* privacy. Tale documentazione, infatti, dovrà essere inviata all'OdC al momento dell'avviso delle attività di verifica e, in via di principio, dovrà comprendere:

- un Modello Organizzativo Privacy. Quest'ultimo, dovendo regolare le procedure e i protocolli relativi gestione della protezione dei dati personali nell'organizzazione aziendale, dovrebbe comprendere: 1. La mappatura dei trattamenti (descrizione dei processi interni, l'analisi degli archivi interni ed esterni, analisi dei rischi); 2. Le istruzioni formali alle persone autorizzate al trattamento sotto l'autorità del titolare (addetti e/o dipendenti); 3. Le qualifiche e contratti con i responsabili, ed eventuali *sub*-responsabili, del trattamento; 4. Le procedure di monitoraggio degli Amministratori di Sistema; 5. *template* di informative (ed eventuali richieste di consenso);
- il Registro delle attività di trattamento;
- le DPIA effettuate e la metodologia di valutazione del rischio del trattamento;
- le procedure che regolano la raccolta e il trattamento, nonché quelle relative alla gestione dei diritti dell'interessato;
- procedure di valutazione delle misure tecniche ed organizzative adottate;
- relazioni finali del DPO e dell'Amministratore di sistema, se nominati;
- procedure di gestione dei data breach ed altri documenti concernenti le condizioni operative del trattamento.

Rispetto all'individuazione delle fonti di rischio e alla gestione delle medesime, i criteri di certificazione, prendendo a riferimento gli artt. 32 e 35 del GDPR, prevedono che il titolare e/o il responsabile del trattamento mettano in atto tutte le misure tecniche ed organizzative utili a prevenire ogni possibile conseguenza pregiudizievole che un trattamento potrebbe generare.

Nel compiere tale valutazione, l'ente richiedente la certificazione deve prendere in considerazioni tutte le variabili di contesto che possono impattare sul trattamento dei dati e tutte le fonti di rischio che possano compromettere la riservatezza, l'integrità, la

[23] Tali macro-processi corrisponderebbero ai principi di quali la liceità del trattamento, la capacità e tempestività di notificare violazioni, la *privacy by design e by default* e la valutazione d'impatto ove applicabile. Cfr. C. CIAMPI, *Certificazioni in ambito GDPR, ecco il nuovo schema ISDP©10003*, in *CyberSecuriti360*, 2020, in Rete: *https://www.cybersecurity360.it/legal/privacy-dati-personali/certificazioni-in-ambito-gdpr-ecco-il-nuovo-schema-isdp10003/*.

disponibilità e la qualità dei dati personali trattati. Inoltre, devono essere qualificati i rischi interni ed esterni, definendo preliminarmente un livello di rischio accettabile e di rischio inerente, mediante parametri oggettivi. A fronte di tali indagini, titolari e responsabili devono valutare se il rischio residuo, raffrontato al valore del rischio accettabile, possa essere considerato controllabile. Se il rischio residuo risulta elevato, il titolare deve procedere, prima di iniziare il trattamento, a compiere una DPIA e, nel caso, a consultare l'autorità di controllo attraverso la procedura di cui all'art. 36 GDPR[24].

Tali verifiche andranno compiute per ogni singolo trattamento oggetto di valutazione per la certificazione e durante tutto il ciclo di vita dello stesso. Il titolare e il responsabile, coadiuvati dal DPO, dovranno, infine, monitorare l'efficacia meno delle misure adottate, procedendo all'eventuale aggiornamento delle misure operative adottate ed inserire la documentazione di verifica nel MOP[25].

Con riferimento ai criteri relativi alla sicurezza del trattamento, il titolare richiedente la certificazione, sulla base del parere 3/2010 del WP29[26], dovrà valutare, attuare, riesaminare e mantenere attivo un opportuno sistema di misure tecniche ed organizzative al fine di garantire un livello di sicurezza adeguato al rischio potenziale che incombe sui dati rispetto alla loro possibile distruzione, perdita, modifica, rivelazione non autorizzata o accesso illecito. Rispetto al responsabile del trattamento, invece, i criteri prevedono che questi assista e collabori con il titolare per l'adempimento degli obblighi di sicurezza e integrità dei dati trattati.

Per raggiungere efficacemente tali scopi il titolare del trattamento dovrebbe definire una strategia di gestione dei rischi operativi connessi al trattamento dei dati effettuato, tenendo conto delle potenzialità della propria struttura e, soprattutto, dei potenziali rischi che incombono sui dati nel trattamento in oggetto. Questa strategia di gestione dovrebbe comprendere tutte le misure organizzative necessarie per gestire adeguatamente i processi, quindi: *policy* operative aziendali e relativa documentazione, meccanismi di segnalazione delle eventuali difformità, formazione e risorse adeguate al personale, *audit* periodici[27].

Riguardo all'adeguatezza dei processi interni la certificazione insiste molto sui principi che titolari del trattamento devono rispettare e, in particolare, che siano rispettati i diritti e le libertà fondamentali degli interessati e predisposti meccanismi di monitoraggio interni al trattamento, anche al fine di individuare possibili errori o

[24] Chiaramente, nel caso in cui il trattamento da certificare corrisponda ad uno fra quelli per cui la DPIA è obbligatoria, ai sensi dell'art. 35 par. 4 GDPR, il titolare del trattamento dovrà necessariamente svolgere la valutazione a prescindere dal livello di rischio da lui individuato. Sul punto, il WP29, con le Linee Guida WP 248 rev.01, ha provveduto ad individuare un elenco comune dell'Unione europea delle tipologie di trattamento per le quali è obbligatorio procedere a una valutazione d'impatto sulla protezione dei dati. Per approfondire v. WP29, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*, 2017, 9-11, in Rete: *https://ec.europa.eu/newsroom/article29/items/611236/en*; GPDP, *Valutazione d'impatto della protezione dei dati (DPIA)*, in Rete: *https://www.garanteprivacy.it/valutazione-d-impatto-della-protezione-dei-dati-dpia-*.

[25] Cfr. INVEO, *ISDP©10003, Schema internazionale per la valutazione della conformità al Regolamento Europeo 2016/679*, *op. cit*., 14-15.

[26] Cfr. WP29, *Parere 3/2010 sul principio di responsabilità, op.cit*.

[27] Cfr. *ivi.*, 15-16.

violazioni di sicurezza. Inoltre, sarà continuativamente necessario verificare che le politiche adottate siano in linea con il principio della *privacy by design* e infine che gli eventuali co-titolari e responsabili del trattamento svolgano correttamente i propri ruoli.

La formazione rappresenta una misura organizzativa fondamentale per la corretta predisposizione della *data protection governance*. Per questo motivo, pur essendo già richiamata in diversi punti, lo schema ISDP©10003 assegna particolare rilievo alla verifica dei processi formativi. Viene previsto che il titolare o il responsabile del trattamento verifichino puntualmente la formazione del proprio personale e attribuendo al DPO, ove nominato, un ruolo di verifica della preparazione delle risorse umane agli adempimenti relativi alla protezione dei dati personali.

Per quanto concerne, invece, l'operatività del controllo e delle operazioni di verifica, la certificazione prevede che il titolare o il responsabile del trattamento debbano predisporre tutta la documentazione necessaria per verificare la soddisfazione dei requisiti di certificazione[28]. Dalle informazioni contenute in questi documenti si desumerà la corrispondenza o meno del trattamento svolto dall'organizzazione da certificare ai criteri di certificazione previsti dalla ISDP©10003. Tali criteri sono individuati nell'allegato finale dello schema, ove vengono elencati i controlli su cui si formeranno le valutazioni e i giudizi dell'OdC. Questi ricomprendono 122 controlli, relativi ai sette macro-processi precedentemente individuati[29]. Tutti i criteri di certificazione previsti dal ISDP©10003 hanno una corrispondenza precisa con gli articoli del GDPR, permettendo di poterli raggruppare in base alla norma di riferimento verso cui collimano. In particolare, vi sono: 8 controlli relativi all'art. 4 (Definizioni); 17 controlli relativi all'art. 5 (Principi del trattamento); 1 controllo relativo all'art. 6 (Liceità del trattamento); 6 controlli relativi all'art. 7 (Condizioni del consenso); 1 controllo relativo all'art. 8 (Consenso dei minori); 9 controlli relativi agli artt. 13-16 (Informativa, Diritto di accesso e Diritto di rettifica); 1 controllo relativo all'art. 18 (Diritto di limitazione di trattamento); 1 controlli relativo all'art. 20 (Diritto alla portabilità); 4 controlli relativi all'art. 24 (Responsabilità del titolare del trattamento); 10 controlli relativi all'art. 25 (DPbDD); 6 controlli relativi all'art. 28 (Responsabile del trattamento); 2 controlli relativi all'art. 29 (Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento); 6 controlli relativi all'art. 30 (Registro delle attività di trattamento); 26 controlli relativi all'art. 32 (Sicurezza del trattamento); 4 controlli relativi agli artt. 33-34 (Segnalazione *data breach*); 7 controlli relativi all'art. 35 (DPIA); 7 controlli relativi agli art. 37-39 (DPO); 5 controlli relativi all'art. 44 (Principio generale per il trasferimento transfrontaliero di dati); 1 controllo relativo all'art. 49 (Deroghe per il trasferimento transfrontaliero)[30].

[28] Cfr. *ivi.*, 18.

[29] A fini esaustivi si riportano nuovamente le sette macrocategorie (processi) di controlli: 1. Politiche e obbligazioni del titolare; 2. Soggetti coinvolti nel processo del trattamento; 3. Principi applicabili al trattamento e tutela dei diritti; 4. Processi di adeguamento in fase di ideazione ed all'atto del trattamento a norma art. 25; 5. Obblighi generali, gestione del rischio e sicurezza dei trattamenti; 6. Valutazione d'impatto; 7. Trasferimento dei dati personali verso paesi terzi, IoT e cloud computing.

[30] Cfr. INVEO, *ISDP©10003, Schema internazionale per la valutazione della conformità al Regolamento Europeo 2016/679*, *op. cit.*, 21-38.

Per l'adesione ad un meccanismo di certificazione, è richiesto che i titolari o i responsabili del trattamento adottino un sistema di monitoraggio efficacie al fine di adottare le misure tecniche ed organizzative ai nuovi o diversi rischi conseguenti al trattamento. Tale criterio è valorizzato anche dallo schema ISDP©10003 il quale richiede ai soggetti richiedenti la certificazione l'aggiornamento, su base continuativa, delle politiche di protezione dei dati personali. In particolare, si prevede che il titolare può conseguire questa verifica attraverso la pianificazione di un programma di *audit* interni od esterni. Lo schema prevede puntualmente gli elementi che titolari e responsabili del trattamento debbano considerare nella fase di monitoraggio, mentre, per quanto riguarda le modalità di valutazione, gli *auditor* dovranno fare riferimento ai requisiti previsti dalla ISO/IEC 17065, dalle Linee Guida 4/2018 dell'EDPB nonché ai requisiti aggiuntivi stabiliti dal GPDP. Tutti questi elementi sono complessivamente finalizzati a migliorare la gestione dei processi interni e, prevalentemente, la gestione del rischio. Ovviamente se la fase di monitoraggio è finalizzata a conseguire miglioramenti nella gestione della protezione dei dati personali, nel caso inverso in cui si riscontrassero dei rilievi [31] nelle fasi di *audit*, il titolare o il responsabile del trattamento dovranno intraprendere le azioni necessarie per eliminare le cause che lo hanno determinato.

Con riguardo al processo di certificazione, Inveo oltre ad essere lo *scheme owner* è altresì accreditata ai sensi della norma ISO/IEC 17065 per la certificazione di prodotti, servizi o processi. Oltre a poter attribuire direttamente i marchi relativi alla certificazione ISDP©10003, Inveo concede, con degli accordi di licenza, ad altri OdC di attribuire la certificazione sulla base dei criteri dello schema. Inoltre, riguardo ai procedimenti di certificazione dalla stessa svolti, questi possono essere effettuati, mediante previo accordo, anche da personale esterno e *auditor* accreditato da Inveo a seguito di un eventuale procedimento di formazione. Infine, rispetto all'assegnazione del marchio di certificazione, questo è subordinato alla sottoscrizione tra Inveo e l'organizzazione da certificare di un contratto di licenza finalizzato a definire le obbligazioni di entrambe le parti, rispetto, ad esempio, allo svolgimento delle verifiche, a disciplinare l'uso autorizzato o meno del marchio, le spese per la licenza del marchio e le condizioni di sospensione o revoca della certificazione prima della scadenza. La valutazione di adeguatezza dell'organizzazione è formata in due fasi: la prima, prettamente documentale, è rivolta a valutare la completezza e la corrispondenza della documentazione dell'organizzazione ai criteri di certificazione; la seconda, invece, concerne la vera e propria ispezione il loco, nel quale si andranno ad analizzare lo stato e l'effettiva implementazione delle misure tecniche ed organizzative richieste dai controlli. Conclusa la fase di verifica la certificazione potrà essere attribuita per una durata di tre anni. Con riguardo al monitoraggio e possibile revoca del marchio di certificazione, lo schema ISDP©10003 non si discosta dalle previsioni del GDPR: il mantenimento del marchio è subordinato al persistente rispetto dei criteri di

[31] Cfr. *ivi*, 19-20. In particolare, lo schema classifica i rilievi riscontrabili in: 1) Non conformità: quando i vari requisiti di riferimento dati dal GDPR vengono costantemente disattesi, mettendo a rischio l'affidabilità del prodotto, processo o servizio; 2) Osservazione: il criterio/principio viene applicato solo parzialmente o disatteso senza però inficiare l'affidabilità del prodotto, servizio o processo oggetto di valutazione; 3) Commento: eventuali irregolarità che non inficiano la capacità del prodotto, servizio o processo oggetto di valutazione di soddisfare i requisiti di riferimento.

certificazione e, su base annuale, viene svolto il relativo controllo sul trattamento certificato. In caso in cui Inveo, o gli altri OdC licenziati, riscontrino delle difformità sull'applicazione della certificazione, l'organizzazione avrà quattro mesi di tempo per rimediare ai rilievi riscontrati. In caso contrario si avrà la revoca.

In conclusione, la certificazione ISDP©10003 può essere considerata un corretto interprete delle obbligazioni previste dal GDPR. Tuttavia, lo stesso, presenta attualmente una criticità. Pur essendo stato riconosciuto dallo studio Tilburg come un meccanismo di certificazione nello scopo dell'art. 42 GDPR, questo non è ancora uno schema ai sensi del GDPR. Infatti, i criteri di certificazione predisposti dallo *scheme owner* non sono ancora stati approvati dall'autorità nazionale competente, ossia il GPDP. Questo determina che, al momento, la certificazione non è valida ai sensi dell'art. 42 GDPR, ma rappresenta comunque uno strumento fondamentale di *accountability* per dimostrare la propria conformità al Regolamento[32]; inoltre, lo schema è stato comunque approvato da Accredia ai sensi del Regolamento (CE) n. 765/2008. Nonostante ciò, è stato recentemente confermato da Inveo che, attualmente, il progetto dei criteri di certificazione è stato consegnato al Garante per la protezione dei dati personali per l'approvazione della certificazione ai sensi dell'art. 42, par. 5 GDPR, comportando che, nel prossimo futuro, la certificazione ISDP©10003 sarà valevole ai sensi del GDPR[33].

3 European Privacy Seal (EuroPriSe©) per la certificazione dei trattamenti di dati personali svolti da responsabili del trattamento

Il secondo meccanismo di certificazione generale per la protezione dei dati personali è il tedesco EuroPrise. Quest'ultimo è stato realizzato durante la vigenza della Direttiva Madre come strumento volontario per attestare la conformità alla normativa *data protection* dei prodotti e servizi IT[34]. Originariamente, lo schema EuroPriSe si distingueva per il fatto che la sua 'legittimità' derivava dalla collaborazione tra le autorità pubbliche europee e nazionali e le organizzazioni del settore privato. La Commissione europea e la Direzione generale delle reti di comunicazione, dei contenuti e delle tecnologie, infatti, hanno sostenuto lo sviluppo della certificazione attraverso il programma eTEN[35]. Inoltre, le autorità di controllo dello stato tedesco dello Schleswig-Holstein (ULD), la CNIL francese e l'APDC spagnola facevano parte del consorzio a sviluppo di EuroPriSe. In ragione della natura degli attori coinvolti, il progetto EuroPriSe

[32] Lo schema, infatti, può ragionevolmente valere come attenuante 'generica' *ex* art. 83, par. 2, lett. k) GDPR, in caso di sanzione da parte dell'autorità di controllo.

[33] Cfr. R. GIANNETTI, *Privacy Day Forum 2023: lo speech di Riccardo Giannetti su Certificazioni & GDPR*, 2023, in Rete: *https://www.youtube.com/watch?v=GmQ7TRvEoqY*.

[34] Cfr. D. SPAGNUELO, A. FERREIRA, G. LENZINI, *Accomplishing Transparency within the General Data Protection Regulation*; in P. MORI, S. FURNELL, O. CAMP (a cura di), *Proceedings of the 5th International Conference on Information Systems Security and Privacy*, 2019, 119, in Rete: *https://pdfs.semanticscholar.org/b1ef/d7ef48255477cfe6d8c81aa613cc18dcd1d0.pdf*.

[35] V. EUROPEAN COMMISSION, *Programma eTEN per la diffusione dei servizi elettronici in Europa*, 2012, in Rete: *https://digital-strategy.ec.europa.eu/en/news/eten-programme*. Il Programma eTen ha supportato lo sviluppo trans-europeo di servizi digitali di pubblico interesse, coprendo diversi temi: eGovernment, sanità digitale, inclusione digitale, formazione e scolarizzazione digitale e servizi per le PMI. Il programma si è concluso al termine del 2006.

è stato sviluppato secondo la disciplina di riferimento europea della DPD, come interpretata dalla giurisprudenza della GCUE e integrata dalle linee guida del WP29/EDPB, e della relativa normativa attuativa tedesca (*Bundesdatenschutzgesetz – Federal Data Protection Act)*[36].

La gestione della certificazione era stata affidata alla ULD dal 2009 al 2014, sino a quando quest'ultima non ha trasferito le operazioni relative alla certificazione ad un organismo privato, ossia la EuroPriSe GmbH[37]. Quest'ultima, quindi, attualmente costituisce lo *scheme owner* dello schema EuroPriSe, gestendo altresì il processo di certificazione e i procedimenti di formazione degli esperti che andranno a condurre le valutazioni sulle organizzazioni che intendono certificarsi.

Come detto, la certificazione EuroPriSe ha ad oggetto prodotti o servizi IT e siti web in cui sia operativo un trattamento dei dati personali[38]. La certificazione assicurerebbe agli utenti che i loro dati personali siano trattati conformemente alla normativa esistente, offrendo adeguate garanzie di trasparenza e chiarezza in merito alla base giuridica del trattamento, soprattutto per quanto riguarda le categorie particolari di dati, al rispetto dei principi *data protection* e ai diritti degli interessati, nonché all'implementazione di misure tecniche ed organizzative adeguate[39]. La finalità di questa certificazione risulta evidente: assicurare i diritti degli interessati e aumentare la fiducia di questi ultimi nei prodotti e servizi della società dell'informazione. Il soffermarsi sulla trasparenza, dunque, mirerebbe a facilitare i coinvolgimenti degli interessati nel mercato dei dati.

Proprio per il mantenimento della sua finalità, dopo l'entrata in vigore del GDPR, la certificazione EuroPriSe ha dovuto subire un adeguamento alla nuova normativa armonizzata sulla protezione dei dati personali. Per tale ragione, i nuovi criteri hanno tratto origine direttamente dai requisiti del Regolamento, traducendone i principi ed obblighi in domande a cui è possibile rispondere nel contesto di un *audit*. Queste domande, quindi, si basano sugli obblighi specificati dal GDPR e le loro risposte determinano la conformità a tali obblighi.

---

[36] Per approfondire la disciplina delle certificazioni privacy nell'ordinamento tedesco v. G. HORNUNG, S. BAUER, *Privacy Through Certification?: The New Certification Scheme of the General Data Protection Regulation*; in P. ROTT (a cura di), *Certification - Trust, Accountability, Liability*; 2019; 109-132; in Rete: *https://link.springer.com/book/10.1007/978-3-030-02499-4*.

[37] Cfr. R. MEDZINI, *Governing the shadow of hierarchy: enhanced self-regulation in European data protection codes and certifications*, In *Internet Policy Review*, v. 10(3), 2021, 10-11, in Rete: *https://doi.org/10.14763/2021.3.1577*. La ragione di tale passaggio è da ricondurre allo scopo di consentire allo schema di progredire in relazione alle nuove tecnologie nel frattempo emergenti. In ogni caso il ULD avrebbe continuato a far parte dell'*advisory board* avente il compito di supervisionare lo sviluppo dello schema e dei criteri di certificazione. Cfr. A. CAVOUKIAN, M. CHIBBA, *Privacy Seals in the USA, Europe, Japan, Canada, India and Australia*, in R. RODRIGUES, V. PAPAKONSTANTINOU (a cura di) *Privacy and Data Protection Seals*, 70-71.

[38] Cfr. EUROPRISE, *Scheme for IT Products and IT based Services*, in Rete: *https://www.euprivacyseal.com/certification-schemes/scheme-for-products-and-services/*.

[39] Cfr. S. BILGESU, *The Certification Mechanism Under the EU General Data Protection Regulation*, 2019, 64, in Rete: *https://www.proquest.com/dissertations-theses/certification-mechanism-under-eu-general-data/docview/2495414321/se-2*; A. CAVOUKIAN, M. CHIBBA, *Privacy Seals in the USA, Europe, Japan, Canada, India and Australia*, *op. cit.*, 70-71.

Nonostante le necessità di aggiornamento al GDPR, la certificazione EuroPriSe "*for the certification of IT products and IT-based services*" è stata comunque valutata dallo Studio Tilburg come uno schema di certificazione rientrante nello scopo degli artt. 42 e 43 del GDPR. Come riscontrato dallo studio, EuroPriSe ricomprende tutti le obbligazioni previste dal Regolamento in un unico schema, rendendone semplice e flessibile l'adesione per le imprese.

La certificazione inizia con un contratto (definito "*evaluation agreement*") tra l'organizzazione che intende certificarsi e l'*auditor* esterno che si occuperà della valutazione di conformità del servizio o prodotto ai criteri di certificazione, senza alcuna interferenza di EuroPriSe. Quest'ultima interviene, invece, per la stipula del contratto di certificazione con l'organizzazione del titolare o responsabile del trattamento, prima della valutazione dell'esperto esterno. Tale contratto è necessario per la definizione del ToE della certificazione nel caso concreto, per la determinazione dei compensi e per la fissazione dei diritti e doveri contrattuali delle parti, quali quello di cooperazione in buona fede nel corso del procedimento di certificazione e nel dovere di riservatezza.

Superata questa fase, gli *auditor* esterni accreditati dall'*advisory board* di EuroPriSe GmbH dovranno verificare la corrispondenza del servizio o prodotto che si intende certificare ai criteri della certificazione; Gli esperti non sostituiscono l'OdC e, quindi, non rilasciano la certificazione. Quest'ultima viene sempre attribuita da EuroPriSe GmbH, il quale però si avvale di questi professionisti, preparati sia nell'ambito di verifica legale sia nell'ambito tecnico, per compiere le valutazioni sulla conformità dell'organismo che intende certificarsi. L'accreditamento di questi *auditor* avviene similmente a quanto previsto dall'43 GDPR: questi devono dar prova della propria competenza e indipendenza e l'accreditamento ha una durata di tre anni, rinnovabile sempre da EuroPriSe GmbH[40].

I criteri di certificazione su cui si basano le valutazioni determinanti l'attribuzione del marchio EuroPriSe colgono, come detto, i principali principi e obblighi di compliance previsti dal GDPR. Oltre a ciò, viene assegnata particolare attenzione: alle misure tecniche ed organizzative introdotte per la protezione dei dati e dei diritti degli interessati; agli specifici requisiti concernenti il prodotto o il servizio IT, in ottica di attuazione del principio della DPbDD; alla corretta esecuzione delle istanze degli interessati per l'esercizio dei loro diritti; alla tutela dei diritti attribuiti dalla Direttiva *ePrivacy*[41].

In tale frangente, i metodi di valutazione potranno includere la richiesta di documentazione, accessi all'organizzazione, interviste con il personale rilevante dell'organizzazione da certificare, l'uso di eventuali versioni di prova del prodotto o servizio da certificare e l'analisi del codice sorgente e della relativa documentazione

[40] Cfr. EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, G. BODEA, K. STUURMAN, M. BREWCZYŃSKA, *Data protection certification mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679: annexes*, *op. cit.*, 47.

[41] Pur potendo essere strutturalmente divisi nella menzionata categorizzazione, all'interno dello schema i criteri di certificazione sono testualmente divisi in quattro *sets* di controlli, a loro volta divisi in *sub*-sets. Questi sono: "Set *1: Overview on Fundamental Issues; Set 2: Legitimacy of Data Processing; Set 3: Technical-Organisational Measures; Set 4: Data Subjects' Rights*". Cfr. EUROPRISE, *EuroPriSe Criteria for certification of IT products and IT-based services*, 2017, 15, in Rete: *https://www.euprivacyseal.com/wp-content/uploads/2023/01/EuroPriSe-Criteria-v201701_final.pdf*.

rilevante [42]. Alla fine di queste operazioni, gli esperti redigeranno un report di valutazione in cui saranno contenute le valutazioni concernenti la conformità dell'organizzazione da certificare ai criteri di certificazione. Quest'ultimo sarà inoltrato al comitato della EuroPriSe, il quale rilascerà il marchio di certificazione dopo aver validato il report di valutazione verificandone la completezza, la coerenza metodologica e la rispondenza ai criteri di certificazione. Concluse tali valutazioni e convalidato il report, EuroPriSe andrà a redigere la relazione di certificazione finale, la quale sarà pubblicata sul sito di EuroPriSe per garantire la trasparenza del processo di certificazione[43]. Proprio a tal fine, EuroPriSe pubblica online il nome e il tipo di servizio o prodotto, la versione dei criteri di certificazione utilizzati durante il processo, la certificazione, il periodo di validità, le date degli *audit* di monitoraggio e i risultati principali della valutazione in un breve rapporto pubblico[44].

Assegnato il marchio di certificazione EuroPriSe, questo ha una durata di due anni, rinnovabile al costante soddisfacimento dei criteri di certificazione previsti, operando gli eventuali adeguamenti necessari per allinearsi all'aggiornamento dello schema.

Attribuita la certificazione, altra importante questione è il sistema di monitoraggio in quanto è necessario per la constante attuazione dei criteri di certificazione e per un tempestivo intervento dell'OdC in caso di difformità. Lo schema di certificazione prevede sul punto che vengano effettuati degli *audit*, mediante accessi, con cadenza regolare o casuale durante il periodo di certificazione, al fine di verificare il perdurante rispetto del soggetto certificato del principio di *accountability*. Questo sistema di *follow-up* effettuato dagli esperti di EuroPriSe GmbH permette di rilevare efficacemente le difformità ai criteri di certificazione, segnalandole alle autorità nazionali di controllo competenti affinché queste adottino, d'ufficio, i provvedimenti ritenuti più idonei a contrastare il trattamento illecito. Questi *audit* fanno sì che le organizzazioni certificate siano vigili sulle loro responsabilità, rendendo possibile supplire ad ogni violazione dei criteri prima che venga causato un danno all'interessato[45].

Oltretutto, nell'eventualità di importanti modifiche tecniche o legali, EuroPriSe potrà richiedere di ricertificare, anticipatamente alla naturale scadenza del marchio, il servizio o il prodotto IT che sia stato oggetto di tali aggiornamenti.

---

[42] Cfr. EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, G. BODEA, K. STUURMAN, M. BREWCZYŃSKA, *Data protection certification mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679: annexes*, *op. cit.*, 47.

[43] Cfr. ENISA, *Recommendations on European Data Protection Certification*, 2017, 33, in Rete: *https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification*.

[44] La pubblicazione di questo report finale è necessaria per promuove la trasparenza della procedura rispetto ai terzi che interagiscono con l'organizzazione certificata. Cfr. R. RODRIGUES, D. BARNARD-WILLS, D. WRIGHT, P. DE HERT, V. PAPAKONSTANTINOU, L. BESLAY, N. DUBOIS, *EU Privacy seals project: Inventory and analysis of privacy certification schemes*, 2013, 40, in Rete: *https://data.europa.eu/doi/10.2788/29861*.

[45] In particolare, gli esperti esterni procederanno a due *audit* di monitoraggio a 8 e 16 mesi dalla positiva conclusione del processo di certificazione o di ricertificazione per verificare il mantenimento dei requisiti di conformità. Se saranno riscontrate delle violazioni, queste verranno notificate all'organizzazione certificata e, se necessario, al comitato di certificazione di EuroPriSe per l'adozione dei provvedimenti opportuni, fra cui la sospensione e la revoca della certificazione. Cfr. EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, G. BODEA, K. STUURMAN, M. BREWCZYŃSKA, *Data protection certification mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679: annexes*, *op. cit.*, 48 *ss*.

Malgrado la sua completezza, la certificazione EuroPriSe per prodotti e servizi informatici non è pienamente conforme all'art. 42 GDPR. Infatti, lo schema ha ad oggetto la valutazione di prodotti o servizi IT, o parti di esse, ove il trattamento di dati personali costituisce un elemento – se non la base – del prodotto, ma non il ToE. Le certificazioni ai sensi dell'art. 42 concernono invece la verifica della conformità di uno o più trattamento (ToE) i quali possono far parte di un prodotto, processo o servizio, in base alla norma ISO/IEC 17065[46].

Infine, altra critica che è stata rivolta ai criteri EuroPriSe per la certificazione di prodotti e servizi IT è la scarsa considerazione all'art. 25, dedicando solo una limitata attenzione ai principi della DPbDD al riguardo del principio di minimizzazione dei dati nel trattamento e nell'adozione di misure di anonimizzazione e/o pseudoanonimizzazione[47].

Per tale ragione, la EuroPriSe GmbH ha definito dei nuovi criteri per la certificazione dei trattamenti svolti da responsabili del trattamento[48]. La certificazione EuroPriSe *"for the certification of processing operations by processors"* rappresenterebbe uno degli strumenti previsti dall'art. 28 GDPR per attestare la conformità al Regolamento di un trattamento svolto da un responsabile del trattamento, al fine di aumentare la fiducia dei titolari del trattamento e degli interessati nel fatto che i propri dati siano trattati correttamente. Qualsiasi organizzazione che tratti dati personali come responsabile del trattamento ai sensi del GDPR può richiedere la certificazione nell'ambito di questo schema. A differenza di quello concernente i prodotti e servizi IT, i criteri di certificazione del meccanismo EuroPriSe per i responsabili del trattamento sono stati approvati dall'organismo nazionale di accreditamento tedesco e dalla LDI-NRW, la Commissione per la protezione dei dati personali e la libertà di informazione dello Stato del Nordrhein-Westfalen[49], come richiesto dalla normativa nazionale tedesca[50]. Inoltre, i criteri di certificazione sono stati portati all'attenzione

[46] La medesima considerazione è espressa anche nel sito *web* di EuroPriSe, ove si evidenzia che: "*this certification scheme does not qualify as an approved certification mechanism in the meaning of Art. 42 GDPR. IT products as such are generally not covered by the scope of application of Art. 42 GDPR*". Cfr. EuroPriSe, *Scheme for IT Products and IT based Services*, in Rete: *https://www.euprivacyseal.com/certification-schemes/scheme-for-products-and-services/*.

[47] Cfr. I.S. RUBINSTEIN, N. GOOD, *The trouble with Article 25 (and how to fix it): the future of data protection by design and default*, in *International Data Privacy Law*, 2020, Vol. 10, No. 1, 53 (37-56), in Rete: *https://doi.org/10.1093/idpl/ipz019*.

[48] Cfr. EUROPRISE, *EuroPriSe Criteria for the certification of processing operations by processors*, 2022, in Rete: *https://www.euprivacyseal.com/wp-content/uploads/2022/12/Kriterien_Verarbeitungsvor gange-von-AV_EN_v3_0.pdf*.

[49] Cfr. LDI-NRW, *LDI NRW genehmigt erste deutsche Kriterien für Datenschutz-Zertifizierung*, 2022, in Rete: *https://www.ldi.nrw.de/ldi-nrw-genehmigt-erste-deutsche-kriterien-fuer-datenschutz-zertifizierung*; BFDI, *The 2022 Activity Report of the Federal Commissioner for Data Protection and Freedom of Information*, 2023, 78, in Rete: *https://www.bfdi.bund.de/SharedDocs /Downloads/EN/Taetigkeitsberichte/31TB_22.pdf?__blob=publicationFile&v=6*. In particolare, i criteri di certificazione sono stati approvati il 7 ottobre 2022, a seguito dei rilievi sollevati dall'EDPB.

[50] Cfr. LDI-NRW, *Sezione pagina web Akkreditierung/Zertifizierung*, in Rete: *https://www.ldi.nrw.de/ datenschutz/wirtschaft/akkreditierungzertifizierung*. In Germania, gli organismi di certificazione sono accreditati dall'ente di accreditamento tedesco (DAkkS) insieme alle autorità di controllo indipendenti dei diversi stati federali in conformità con il paragrafo 39 BDSG. Inoltre, gli OdC dovranno rispettare i requisiti supplementari alla norma ISO/IEC 17065 stabiliti dalla Conferenza sulla protezione dei dati (DSK).

dell'EDPB, in base al meccanismo di cooperazione, ai fini dell'approvazione come Sigillo europeo per la protezione dei dati personali[51].

Come per la precedente certificazione per i prodotti e servizi IT, i criteri di certificazione dello schema EuroPriSe per i responsabili del trattamento sono pubblicati sul sito web della EuroPriSe GmbH, rendendo più semplice per le organizzazioni che intendono aderire alla certificazione determinare a quali requisiti devono sottostare e verificare il quadro del proprio sistema di *compliance* nell'ottica di adeguarlo a quanto previsto dai criteri.

I criteri di criteri di certificazione sono formulati sotto forma di domande a cui gli esperti esterni, chiamati ad accertare la conformità dell'organizzazione che intende certificarsi, dovranno rispondere. In particolare, questi ultimi si dividono in tre macrocategorie.

La prima macrocategoria dei criteri di certificazione intende analizzare i requisiti del trattamento da una 'prospettiva legale', da intenderli quale il soddisfacimento delle incombenze formali e di principio previste dal GDPR.

In particolare, si prendono preliminarmente in considerazione i requisiti generali per i responsabili del trattamento, quali la tenuta del Registro dei trattamenti, la nomina del DPO, la designazione del rappresentante dello stabilimento europeo e la cooperazione con le autorità nazionali di controllo[52]. In secondo luogo, si dà spazio ai criteri relativi al rapporto tra il titolare e responsabile del trattamento ai sensi dell'art. 28 GDPR: predisposizione di clausole contrattuali in linea con l'art. 28; corretta implementazione dei doveri contrattualmente stipulati: responsabilità, processi, istruzioni di lavoro. Il responsabile, quindi, dev'essere in grado di dimostrare il fatto che opera in linea con le istruzioni impartite dal titolare del trattamento, ponendo in essere tutte le misure tecniche ed organizzative per assicurare la conformità al Regolamento[53]. Successivamente, gli *audit* dell'OdC interesseranno i requisiti dettati dall'art. 28 GDPR in relazione al rapporto tra il responsabile e gli altri sub-responsabili del trattamento che siano stati ingaggiati. In particolare, il responsabile dovrà selezionare gli altri sub-responsabili tenendo conto del rispetto delle garanzie adeguate alla tutela dei diritti e libertà degli interessati e stipulare con questi ultimi un *data protection agreement*, disciplinante le istruzioni delle attività che il sub-responsabile dovrà svolgere e i relativi obblighi per la protezione dei dati personali[54]. Infine, vengono presi in considerazione il rispetto, da parte dell'organizzazione del responsabile del trattamento che intende certificarsi, di eventuali requisiti settoriali determinati da specifici trattamenti di dati personali, nonché il rispetto dei principi della *data protection by design* e *by default*[55].

Nella seconda macrocategoria di criteri, invece, si tiene conto delle misure tecniche ed organizzative attuate dal responsabile del trattamento per rispondere in

[51] Fatto poi non avvenuto, v. *infra* 121.

[52] Cfr. EUROPRISE, *EuroPriSe Criteria for the certification of processing operations by processors*, *op. cit.*, 6-11.

[53] Cfr. *ivi*, 12-18.

[54] Cfr. *ivi*, 19-25;

[55] Cfr. *ivi*, 26-34. In particolare, rispetto ai particolari trattamenti presi in considerazione, la certificazione si rapporta al rispetto degli obblighi di segretezza professionale (quale quella medica o forense) e al rispetto degli obblighi di segretezza e riservatezza non legalmente disciplinati, quali il *know-how* industriale, brevetti e informazioni riservate in genere.

maniera effettiva al principio di *accountability* e per tutelare i diritti degli interessati. A titolo puramente esemplificativo, vengono analizzate le misure previste dal responsabile per prevenire accessi non autorizzati ai dati o ai programmi e dispositivi che sfruttano i medesimi, le modalità di accesso ai dati personali, i mezzi di cifratura e di anonimizzazione (o pseudoanonimizzazione), le misure per prevenire la perdita accidentale di dati e per assicurarne la disponibilità, nonché le misure di gestione della *cybersecurity* e della riservatezza[56]. Infine, parallelamente alla certificazione EuroPriSe per i prodotti e sistemi IT, vengono presi in considerazione anche le misure adottate dal responsabile del trattamento per rispondere alle istanze di esercizio dei diritti degli interessati.

La terza macrocategoria dei criteri di certificazione concerne le modalità di gestione dei diritti degli interessati e, in particolare, il diritto all'informativa, il diritto di accesso, il diritto di rettificazione, il diritto alla cancellazione o deindicizzazione, diritto di limitazione del trattamento, diritto alla portabilità dei dati e il diritto di opposizione[57].

Con riguardo al processo di certificazione, questo si sviluppa in diverse fasi che coinvolgono differentemente l'OdC, gli esperti dediti alla verifica della conformità e l'organizzazione del responsabile del trattamento. È importante considerare anche che, prima di accedere alla procedura di certificazione, l'organizzazione che intende certificarsi dovrà intraprendere un percorso di autovalutazione della propria conformità al GDPR, in modo da adottare quel procedimento di adeguamento necessario per raggiungere gli standard richiesti dalla certificazione.

Conclusa tale fase, il processo di certificazione si sviluppa come segue:

- in primo luogo, l'organizzazione che intende certificarsi dovrà stipulare un contratto di certificazione con EuroPriSe;
- in secondo luogo, un *team* di esperti svolgerà le verifiche tecniche e legali per l'individuazione del ToE e per l'assunzione della documentazione del responsabile del trattamento; successivamente, un ulteriore team di valutazione verificherà che le informazioni raccolte precedentemente dagli *auditor* e le risultanze delle loro analisi siano corrette[58];
- infine, sulla base dei risultati di verifica e delle conclusioni dei gruppi di esperti, l'OdC compie la decisione sul conferimento della certificazione, assegnando il marchio EuroPriSe quando tutti i criteri di certificazione siano soddisfatti.

Ove quest'ultimo assegnasse il marchio di certificazione all'organizzazione del responsabile del trattamento, questa viene inserita nel registro delle certificazioni attribuite. La certificazione è valida per tre anni, con possibilità, alla scadenza, di rinnovare la certificazione alle medesime condizioni.

Con riguardo al monitoraggio, durante il periodo di validità della certificazione l'OdC svolgerà la necessaria attività di sorveglianza per verificare il constante rispetto dei criteri di certificazione. Eventuali ispezioni, accessi o richieste potranno essere svolte

[56] Cfr. *ivi*, 35-49.

[57] Cfr. *ivi*, 50-54.

[58] Cfr. EUROPRISE, *EuroPriSe Criteria for the certification of processing operations by processors*, in Rete: *https://www.euprivacyseal.com/certification-schemes/scheme-for-processors/*. Nello specifico, l'attività di verifica degli esperti dell'OdC si ispira al c.d. "*four-eyes-principle*". Per approfondire v. *Collaboration in Research and Methodology for Official Statistics. Four eyes principle*, 2019, in Rete: *https://cros-legacy.ec.europa.eu/content/four-eyes-principle_en*.

potenzialmente una volta all'anno senza alcun preavviso, ad eccezione degli anni in cui viene attuata una procedura di ricertificazione (perché, ad esempio, sono mutati i criteri tecnici o legali di riferimento della certificazione). Inoltre, azioni di monitoraggio occasionale potranno essere svolte in caso di anomalie che diano adito a segnalazioni di non conformità ai requisiti di certificazione[59].

3.1 L'intervento dell'EDPB: Opinion 25/2022 riguardo ai criteri di certificazione European Privacy Seal (EuroPriSe) per la certificazione dei trattamenti effettuati dai responsabili del trattamento

Come precedentemente anticipato, i criteri di certificazione EuroPriSe per la certificazione dei responsabili del trattamento, sono stati portati all'attenzione dell'EDPB. Ciò in ragione del fatto che l'art. 64, par. 1, lett. c) prevede che il progetto di decisione per l'approvazione dei criteri di certificazione sia comunicata dall'autorità di controllo nazionale, in questo caso la LDI-NRW, la Commissione per la protezione dei dati personali e la libertà di informazione dello Stato del Nordrhein-Westfalen, all'EBPB per il rilascio di un parere che assicuri l'uniforme applicazione del GDPR all'interno dell'Unione tramite l'applicazione del meccanismo di coerenza.

Pertanto, il 13 settembre 2022 il Comitato si è espresso con l'*Opinion* 25/2022 *regarding the European Privacy Seal (EuroPriSe) certification criteria for the certification of processing operations by processors*, ponendo diversi interrogativi e sollevando varie critiche rispetto alla medesima certificazione[60].

In primo luogo, infatti, il Comitato ha sottolineato come l'ambito territoriale della certificazione non fosse sufficientemente chiaro, in quanto nel titolo del documento relativo ai criteri si dà conto di come la certificazione EuroPriSe sia applicabile solo in Germania, tuttavia, il nome della certificazione è *European Privecy Seal* (certificazione europea sulla privacy). Questa commistione di terminologie potrebbe creare confusione al consumatore o al terzo, pregiudicando, di fatto, l'obiettivo fondamentale che le certificazioni dovrebbero raggiungere, ossia la trasparenza e la chiarezza[61].

Sempre rispetto all'apparente applicazione *extra*-europea, il *Board* ha sottolineato la scarsa chiarezza anche del criterio concernente la nomina di un rappresentante del responsabile del trattamento risiedente in uno stato terzo, per lo stabilimento sito nell'UE. Ciò solleva dubbi in quanto sembrerebbe far intendere che la certificazione EuroPriSe sia applicabile anche per le organizzazioni esterne all'Unione europea le quali trattino dati di interessati appartenenti all'Unione. Tuttavia, così non è, pertanto, il Comitato ha suggerito di specificare e chiarificare la portata applicativa della certificazione. I titolari del trattamento, a prescindere dalla presenza del sigillo di

[59] Cfr. *ibidem.*

[60] Cfr. EDPB, *Opinion 25/2022 regarding the European Privacy Seal (EuroPriSe) certification criteria for the certification of processing operations by processors*, 2022, in Rete: *https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-252022-regarding-european-privacy-seal_en*.

[61] Cfr. *ivi,* 5. L'EDPB, inoltre, ha inteso sottolineare come la certificazione EuroPriSe non fosse una certificazione ai sensi dell'art. 46, par. 2, lett. f) per il trasferimento transfrontaliero di dati personali, in quanto non assicura appropriate garanzie in linea con il *framework* per il trasferimento transfrontaliero di dati.

certificazione, dovrebbero sempre effettuare una valutazione della legislazione del paese ospitante prima di trasferire i dati al responsabile del trattamento – stabilito al di fuori dell'UE – certificato ai sensi del GDPR[62]. Nel caso in cui la legislazione non preveda un adeguato livello di protezione, dovrebbero essere adottate misure supplementari a tutela dei diritti degli interessati o non trasferire i dati nel Paese terzo[63].

In secondo luogo, rispetto alla seconda macrocategoria di criteri relativi all'art. 28 GDPR, e in particolare ai rapporti tra responsabile e titolare del trattamento, il *Board* ha riscontrato diversi controlli generici e/o corrispondenti al testo dell'articolo in questione. Sul punto, quindi, viene sollecitata la specificazione ulteriore dei requisiti e, in particolare, delle misure che il responsabile dovrebbe o potrebbe adottare per l'adempimento dei propri oneri di collaborazione con il Titolare del trattamento. Data l'importanza delle singole posizioni, precisare i compiti operativi del titolare e responsabile del trattamento dovrebbe essere compito degli *scheme owner*, i quali, attingendo dalla prassi e dall'esperienza e competenza degli esperti reclutati, possono permettere lo sviluppo di principi operativi in linea con le norme del GDPR[64], fornendo esempi e modelli.

Rispetto ai criteri concernenti le misure che il responsabile dovrebbe adottare per il trasferimento transfrontaliero di dati personali, il Comitato ne ha evidenziato la genericità, sottolineandone la non verificabilità, con la conseguenza che i medesimi potrebbero portare ad una disomogenea applicazione dello schema di certificazione. Con ciò, nel proprio parere, l'EDPB ha sottolineato come le previsioni relative ai controlli per i trasferimenti transfrontalieri non fossero sufficienti, rendendosi necessaria l'adozione di un approccio più specifico nella definizione dei criteri per l'adozione di misure e garanzie adeguate al trasferimento presso Paesi terzi[65].

Come precedentemente sottolineato, i criteri EuroPriSe prendono in considerazione le misure tecniche ed organizzative implementate dall'organizzazione del responsabile del trattamento per l'attuazione dei principi della DPbDD. Tali criteri, sottolinea il *Board*, necessitano di maggiore precisione, soprattutto rispetto a quanto, alcuni di tali controlli, non devono essere applicabili. La chiarezza e l'esaustività dei criteri di certificazione rappresenta un punto critico frequentemente sottolineato,

[62] Cfr. *ivi*, 6.

[63] Cfr. *ivi*, 8. Le medesime considerazioni vengono svolte anche dal Comitato, il quale raccomanda di precisare: "*in section 2.4.2 that the EuroPriSe certification scheme itself is not a transfer instrument according to Article 46(2)(f) of the GDPR, as it does not provide appropriate safeguards within the framework of transfers of personal data to third countries or international organisations under the terms referred to in letter (f) of Article 46(2)"*.

[64] Cfr. *ivi*, 7. La medesima considerazione viene svolta con riferimento agli oneri documentali dei responsabili del trattamento. I criteri di certificazione, infatti, in diversi punti, richiedono che il responsabile del trattamento fornisca tutte le informazioni necessarie per dimostrare la *compliace* all'art. 28 GDPR, senza, però, specificare quali informazioni o documenti siano necessari. Sul punto, quindi, il *Board* ha sottolineato la scarsa chiarezza ed eccessiva vaghezza del requisito, richiedendo maggiore precisione allo *scheme onwer* nella redazione dei criteri (e conseguentemente nell'individuazione della documentazione necessaria).

[65] Cfr. *ivi*, 9 e 12.

rendendo necessario un adeguamento del modello di certificazione e negli obblighi da soddisfare per essere aderente allo stesso[66].

In conclusione, l'EDPB, pur valorizzando positivamente lo sviluppo generale dei criteri EuroPriSe, considera, tuttavia, che questi ultimi possano portare a un'applicazione incoerente del GDPR e rendendosi necessario apportare diverse modifiche al fine di soddisfare i requisiti imposti dall'articolo 42 del GDPR alla luce delle Linee Guida 1/2018.

Il parere negativo del *Board* non ha comunque interrotto l'approvazione dei criteri EuroPriSe. Infatti, i rilievi sollevati sono stati corretti da EuroPriSe GmbH, consentendo la successiva convalida dei criteri di certificazione da parte dell'autorità di controllo dello Stato del Nordrhein-Westfalen.

4 CNPD – GDPR Certified Assurance Report Based Processing Activities (GDPR-CARPA)

Il GDPR-CARPA è stato redatto e approvato dall'Autorità per la protezione dei dati del Lussemburgo (*Commission Nationale Pour La Protection Des Données, CNPD*) il 13 maggio 2022, dopo l'asseverazione da parte del Comitato europeo per la protezione dei dati con il Parere 1/2022. Il Lussemburgo, è stato, dunque, il primo Paese membro ad approvare un meccanismo di certificazione ai sensi del GDPR a livello nazionale. Imprese, pubbliche amministrazioni e altre organizzazioni stabilite in Lussemburgo hanno la possibilità di aderire alla certificazione GDPR-CARPA per dimostrare la conformità dei propri trattamenti[67]. Infatti, la creazione di un modello di conformità 'accreditato' in base ad una certificazione rappresenta un fattore chiave affinché gli interessati ripongano la propria fiducia nel trattamento dei dati personali coperti dal sistema di certificazione.

Lo sviluppo della certificazione GDPR-CARPA è da attribuire alla collaborazione e agli scambi che il CNPD ha intrattenuto con *auditor* professionisti sin dall'entrata in vigore del Regolamento. La visione di prospettiva determinate dall'unione delle competenze tra l'autorità controllore e gli organismi di valutazione ha, dunque, portato allo sviluppo della prima versione della certificazione. Successivamente, le altre autorità europee per la protezione dei dati hanno esaminato questi criteri nell'ambito del meccanismo di coerenza e, in conclusione, il Comitato Europeo per la protezione dei dati ha emesso il suo parere formale su GDPR-CARPA[68].

L'unicità di tale certificazione è determinata dal fatto che, non solo è stata la prima ad essere approvata ai sensi dell'art. 42, par. 5 del Regolamento, ma è anche l'unica certificazione ad essere interamente sviluppata da un'autorità nazionale di controllo. Allo stato attuale, quindi, la CNPD è lo *scheme owner* del meccanismo di certificazione.

---

[66] Cfr. *ivi*, 9-10. Inoltre, con riferimento all'obbligo del responsabile di sviluppare un modello per l'acquisizione del consenso, l'EDPB ha raccomandato di eliminarlo in ragione dell'eccessiva onerosità dell'obbligo per i soggetti che intendono certificarsi. Infatti, l'acquisizione lecita del consenso non è responsabilità del responsabile del trattamento, ma del titolare; pertanto, è non è coerente attribuire tale onere al responsabile del trattamento allo scopo di dimostrare la *compliance* al GDPR.

[67] Cfr. EDPB, *The CNPD adopts the certification mechanism GDPR-CARPA*, 2022, in Rete: *https://ed pb.europa.eu/news/national-news/2022/cnpd-adopts-certification-mechanism-gdpr-carpa_en*.

[68] Cfr. *ibidem*.

Nel precedente capitolo si è dato conto del fatto che il Regolamento non preveda espressamente la possibilità che le autorità di controllo sviluppino i propri meccanismi di certificazione ai sensi del GDPR. La pubblicazione del GDPR-CARPA costituisce, perciò, un *unicum* nel panorama delle certificazioni relative alla protezione dei dati personali. Infatti, fino ad oggi, il ruolo delle autorità pubbliche era concentrato in una collaborazione con gli enti privati nello sviluppo delle certificazioni privacy e, nonostante alcune ipotesi di certificazioni interamente prodotte da autorità di controllo, questo avveniva nella totale assenza di previsioni normative che disciplinassero la materia certificativa. Di fronte a tale contesto, con il GDPR si è inteso disciplinare organicamente i meccanismi di certificazione relativi alla protezione dei dati personali attribuendo agli organismi pubblici un ruolo di incoraggiamento della prassi nell'elaborazione di tali meccanismi co-regolatori. È per tale ragione che lo sviluppo autonomo di certificazioni da parte delle autorità di controllo, e in particolare la pubblicazione del GDPR-CARPA, ha suscitato diverse critiche, sia dal punto di vista normativo che sistematico.

Nello specifico, seguendo una lettura più rigida del Regolamento, l'art. 42, par. 5 attribuirebbe alle autorità di controllo il compito esclusivo di approvare i criteri di certificazione senza autorizzarle a redigerli autonomamente, sviluppando uno schema proprio.

Su tale interpretazione della norma, inoltre, insisterebbe la critica di natura sistematica rivolta alla possibilità delle autorità di controllo di realizzare meccanismi di certificazione. Ammettendo tale opzione, infatti, si creerebbe un potenziale conflitto di interessi tra il ruolo delle autorità garanti quali OdC, e quindi come enti preposti a verificare la conformità delle organizzazioni richiedenti a dei criteri di certificazione, e la loro veste di autorità investigative preposte alla corretta attuazione del GDPR e alla repressione di eventuali trattamenti illeciti[69].

Rispetto a tale critica, l'interpretazione fornita dell'EDPB e la stesura della certificazione GDPR-CARPA rappresentano delle alternative interpretative assolutamente condivisibili. Il Comitato prevede espressamente nelle Linee Guida 1/2018 che "*quando agisce come organismo di certificazione un'autorità di controllo dovrà garantire la corretta istituzione di un meccanismo di certificazione e sviluppare i propri o adottare criteri di certificazione*" [70], ammettendo la possibilità che le autorità di protezione dei dati personali sviluppino i propri schemi di certificazione. Rispetto al GDPR-CARPA, invece, il CNPD ha superato tale criticità delegando interamente il processo di certificazione a organismi terzi accreditati e concentrarsi solamente all'aggiornamento e stesura dei criteri di certificazione. L'Autorità lussemburghese, quindi, non potrà assegnare personalmente la certificazione, rimanendo esterna rispetto al medesimo procedimento, con solo l'eventuale possibilità di supportare le valutazioni dell'OdC[71]. La CNPD, comunque, mantiene il proprio ruolo di controllo e

[69] Cfr. E. LACHAUD, *What GDPR tells about certification*, in *Computer Law & Security Review*, V. 38, 2020, in Rete: *https://doi.org/10.1016/j.clsr.2020.105457*.

[70] Cfr. EDPB, *Linee Guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione*, *op. cit*., 8.

[71] Il CNPD, infatti, può emettere un parere sulla corretta attuazione, nel caso concreto, dei criteri di certificazione. La valutazione finale sulla conformità dell'organismo da certificare rimane comunque rimessa all'OdC il quale, eventualmente, si avvarrà del parere dell'autorità per un'interpretazione

monitoraggio, per la possibile revoca o sospensione della certificazione o dell'accreditamento.

Come anticipato, l'ambito di applicazione dello schema di certificazione GDPR-CARPA è molto ampio: il meccanismo, infatti, è progettato per rispondere alla necessità dei titolari e responsabili del trattamento di attuare misure tecniche ed organizzative adeguate a garantire la protezione dei dati. Con la necessità di rispondere a tale esigenza, la certificazione è progettata per essere flessibile, non concentrandosi su un campo o un trattamento specifico, ma risultando applicabile in vari settori. Tuttavia, stante la sua genericità, il GDPR-CARPA non risulta adatto a certificare alcuni trattamenti particolarmente specifici[72]. Ciononostante, nulla toglie che, anche in questo campo, la certificazione lussemburghese possa essere uno strumento adatto a dimostrare, parzialmente, la propria *compliance* al GDPR.

I criteri di certificazione sono strutturati in tre sezioni concernenti la *data governance* dell'organizzazione, i principi applicabili al titolare del trattamento e i criteri applicabili al responsabile del trattamento. A prefazione dei criteri di certificazione, inoltre, sono stati predisposti in dettaglio i principi in base ai quali individuare il ToE.

Partendo proprio da quest'ultima sezione, vi è da ribadire che l'obiettivo del GDPR-CARPA è dimostrare la conformità al GDPR delle operazioni di trattamento da parte di titolari e responsabili del trattamento. Sulla base di ciò, spetta all'entità da certificare definire le attività di trattamento nel *target of evaluation*, relative alle operazioni di trattamento coperte dall'oggetto della certificazione. A tal fine, le attività di trattamento sottoposte a verifica devono essere identificate e designate mediante un elenco completo di tutti i sistemi, interfacce (interne ed esterne) e sistemi di archiviazione (elettronici e/o fisici) utilizzati per svolgere tale attività di trattamento. Inoltre, per comprendere appieno le operazioni di trasformazione e manipolazione dei dati, si è rivelato utile distinguere almeno quattro diversi livelli di componenti significativi che influenzano la valutazione delle operazioni di trasformazione: definire l'organizzazione interessata e il suo specifico ecosistema giuridico; definire le circostanze e le finalità del trattamento; definire l'applicazione funzionale utilizzata per implementare le finalità sopra indicate; definire l'infrastruttura informatica utilizzata per tale trattamento[73].

Seguono, quindi, i criteri di certificazione.

---

autentica dei criteri. Questo ulteriore atto 'istruttorio' è permesso in ragione del fatto che il GDPR-CARPA è stato sviluppato sulla base dello schema ISAE 3000 *Type* 2.

[72] Cfr. CNPD, *Le schéma de certification "GDPR CARPA"*, 2023, in Rete: *https://cnpd.public.lu/fr/professionnels/outils-conformite/certification/gdpr-carpa.html*. Come evidenziato dal CNPD, a certificare il trattamento dei dati personali rivolto specificamente ai minori di 16 anni, le attività di trattamento nel contesto di una co-titolarità di trattamento, le attività di trattamento rientranti nell'alveo dell'art. 10 del GDPR e, infine, quelle organizzazioni che non hanno designato un responsabile della protezione dei dati personali (DPO).

[73] Cfr. CNPD, *Décision N° 15/2022 - GDPR Certified Assurance Report based Processing Activities Certification Criteria (GDPR-CARPA), V. 1 / 2022* (d'ora in poi *GDPR-CARPA Certification Criteria*), 2022, 9, in Rete: *https://cnpd.public.lu/dam-assets/fr/professionnels/certification/decision-n-15-2022-du-13-mai-2022-criteres-de-certification.pdf*; CNPD, *GDPR-Certified Assurance Report based Processing Activities Certification Criteria* (d'ora in poi *Schema illustrativo GDPR-CAPRA)*, 2018, 10, in Rete: *https://cnpd.public.lu/dam-assets/fr/professionnels/certification/GDPR-CARPA-Criteria-for-certification-v10.pdf*.

La prima sezione dei criteri concerne la *data governance* all'interno delle organizzazioni richiedenti la certificazione, indipendentemente dalla qualifica di titolare del trattamento o di responsabile del trattamento. Lo scopo di questi criteri è di verificare come i dati personali siano trattati in un'organizzazione dal punto di vista del principio di *accountability*.

Pertanto, i criteri rivolgono la loro attenzione alle *policies* e alle procedure sviluppate dal titolare o responsabile del trattamento, ossia tutte quelle misure organizzative attuate dal richiedente per rispondere alla protezione dei dati, quali: la formale allocazione dei ruoli e responsabili privacy o la previsione di un meccanismo di segnalazione di ogni incidente connesso alla protezione dei dati o ogni violazione del GDPR. Tali procedure devono essere costantemente (almeno su base annuale) riviste e aggiornate tenendo conto, se nel caso, del parere del DPO sul contenuto di esse[74].

Viene richiesto che il richiedente abbia predisposto un Registro delle attività dei trattamenti, a norma dell'art. 30 GDPR, per tutte le categorie di trattamenti nello scopo della certificazione. Anche per il registro ne è previsto il costante aggiornamento, almeno con cadenza annuale, salvo il caso di modifiche dei trattamenti effettuati, al fine di assicurare la completezza e l'accuratezza di ogni record. Tale modifica deve essere documentata e, nell'ambito del processo di certificazione, l'OdC dovrebbe verificare che tutte le informazioni richieste siano accurate, aggiornate e complete per ciascuna attività di trattamento che rientra nell'ambito di applicazione.

Inoltre, l'ente richiedente la certificazione deve adottare misure per garantire che: sia stato designato un punto di contatto per ricevere le richieste degli interessati per l'esercizio dei propri diritti di cui agli artt. 15-22 del Regolamento. Le varie richieste devono essere registrare e la loro esecuzione dev'essere documentata[75].

I controlli continuano verificando la corretta designazione di un DPO nell'organizzazione del soggetto da certificare, appurandone la nomina, o meno (in particolare il richiedente dovrà dar conto dei motivi per cui non è stato nominato), le competenze, la sua posizione nell'organizzazione (verificandone l'indipendenza e assicurando l'assenza di conflitti di interessi con altre posizioni nell'organizzazione del soggetto da certificare), il possesso di adeguate risorse per svolgere i propri compiti, il suo coinvolgimento tempestivo in tutte le questioni relative alla protezione dei dati personali e i suoi compiti (fra cui quelli formativi per le risorse umane del titolare o responsabile da certificare)[76].

Infine, vi sono i criteri relativi alla gestione ed eventuale notifica dei *data breach* e all'implementazione di misure tecniche ed organizzative effettive per prevenire e rilevare (ad esempio istituendo un registro dei *data breach*).

Passando alla seconda sezione, i criteri per il titolare del trattamento intendono verificare l'aderenza del trattamento da certificare ai principi della protezione dei dati

[74] Cfr. CNPD, *GDPR-CARPA Certification Criteria*, *op. cit.*, 9-10.

[75] Cfr. CNPD, *GDPR-CARPA Certification Criteria*, *op. cit.*, 13-14; CNPD, *Schema illustrativo GDPR-CAPRA*, *op. cit.*, 13; J.T. HELMKE, H. LINK, H.H. SCHILD, *Zertifizierungskriterien für Verarbeitungstätigkeiten*. In *Datenschutz Datensich*, Vol. 47, 2023, 102–103, in Rete: *https://doi.org/10.1007/s11623-023-1725-9*.

[76] Cfr. CNPD, *GDPR-CARPA Certification Criteria*, *op. cit.*, 14-17; CNPD, *Schema illustrativo GDPR-CAPRA*, *op. cit.*, 12-13.

personali. Per questa ragione, tale sezione è sezionata in diverse suddivisioni per ogni principio analizzato.

Con il primo *set* di criteri (liceità e trasparenza) si andrà a identificare la base giuridica del trattamento e ad analizzare le condizioni di esercizio della medesima[77]. Successivamente, il documento del CNPD elenca tutti i requisiti per le varie basi giuridiche del trattamento richiamando, sostanzialmente, le formulazioni giuridiche del GDPR e dei vari considerando e, infine, viene dedicata attenzione al trattamento di categorie particolari di dati e sul fatto che il richiedente deve adottare misure adeguate a garantire che tali dati non siano trattati fintantoché non viene individuata una base giuridica valida ai sensi dell'art. 9, par. 2 GDPR[78]. Dopo i criteri relativi alla base giuridica del trattamento, seguono quelli dedicati alle misure di trasparenza che l'ente che intende certificarsi deve adottare. Questi concernono principalmente la disponibilità di informazioni sul trattamento da riferire agli interessati, alla gestione delle istanze di esercizio dei diritti di questi ultimi e sulle modalità di contatto con il titolare o il responsabile del trattamento (o il DPO). È importante evidenziare che la certificazione distingue gli oneri informativi a seconda del fatto che il trattamento sia di natura diretta o indiretta, prevedendo espressamente, in quest'ultimo caso, che l'interessato sia contattato, in tempi ragionevoli, per ricevere ogni informazione necessaria relativa al trattamento e alle possibilità di esercizio dei propri diritti[79]. Infine, seguono i controlli per il trasferimento transfrontaliero di dati personali in paesi terzi, i quali, in sintesi, prevedono che l'organizzazione richiedente la certificazione abbia una base giuridica valida per il trasferimento, che verifichi la sussistenza di rischi per i diritti e le libertà dell'interessato e che adotti una o più delle misure di cui all'art. 46 GDPR per limitare questi rischi.

Le successive sottosezioni dei criteri si agganciano ai principi contenuti nell'art. 5 GDPR: limitazione delle finalità, minimizzazione dei dati, limitazione della conservazione e accuratezza. Particolare riferimento viene fatto alle misure organizzative adottabili per conformarsi a questi principi, quali, ad esempio, la predisposizione di sistemi di *policy* approvati dal DPO, il costante riesame del trattamento per verificare la quantità di dati necessari e l'aderenza del trattamento alle finalità, adottare un sistema di valutazione

[77] A fronte di ciò, il titolare del trattamento dovrebbe adottare misure per garantire che una base giuridica valida per ciascun trattamento sia, prima che adottata, correttamente identificata. Inoltre, vengono specificati gli aspetti di cui l'organismo responsabile deve tener conto nel determinare una base giuridica. Ciò include le finalità perseguite, le circostanze del trattamento (natura, contesto, ambito), un'analisi delle limitazioni del trattamento e delle condizioni stabilite dalla legge, per cui potrebbero essere necessarie ulteriori misure tecniche organizzative. Cfr. CNPD, *GDPR-CARPA Certification Criteria*, *op. cit.*, 14-17; CNPD, *Schema illustrativo GDPR-CAPRA*, *op. cit.*, 16-19; J.T. HELMKE, H. LINK, H.H. SCHILD, *Zertifizierungskriterien für Verarbeitungstätigkeiten*, *op. cit.*, 103-105.

[78] Cfr. CNPD, *GDPR-CARPA Certification Criteria*, *op. cit.*, 25-26; CNPD, *Schema illustrativo GDPR-CAPRA*, *op. cit.*, 16; J.T. HELMKE, H. LINK, H.H. SCHILD, *Zertifizierungskriterien für Verarbeitungstätigkeiten*, *op. cit.*, 103-104.

[79] Cfr. CNPD, *GDPR-CARPA Certification Criteria*, *op. cit.*, 31-38; CNPD, *Schema illustrativo GDPR-CAPRA*, *op. cit.*, 16-19. Inoltre, i criteri di certificazione descrivono dettagliatamente le procedure per l'esercizio di alcuni diritti, quali: il diritto di opposizione, il diritto alla limitazione del trattamento, il diritto di rettifica e il diritto a non essere sottoposto a decisioni basate su trattamenti automatizzati.

delle fonti da cui vengono reperiti i dati e la predisposizione di una procedura per l'esercizio del diritto di rettifica[80].

Infine, l'ultima sottosezione riguarda l'attuazione dei principi di integrità, disponibilità e riservatezza, in cui sono ricompresi i criteri relativi alla sicurezza del trattamento, alla DPIA e sull'affidamento del trattamento ad un responsabile. L'elemento principale di questi criteri riguarda la valutazione del rischio concernente il trattamento. Precisamente, dovranno essere adottate misure per identificare, analizzare e classificare i rischi connessi a qualsiasi trattamento di dati ai diritti e libertà degli interessati. È importante sottolineare che i criteri dovranno essere soddisfatti presentando la documentazione della procedura di valutazione e individuazione dei rischi. Anche le misure di sicurezza dell'organismo richiedente la certificazione sono incluse nelle valutazioni dei criteri, come l'organizzazione della sicurezza informatica, la formazione dei dipendenti, la presenza di controlli di accesso (e salvataggio dei relativi file di *log*) e l'utilizzo di sistemi di *backup* e *recovery* dei dati, sia fisici che digitali. La pianificazione e l'implementazione di queste misure dovrà essere supervisionata anche dal DPO, il quale andrà coinvolto per valutare l'adeguatezza di queste. Sia la valutazione dei rischi che le misure tecniche ed organizzative adottate per attenuarli dovranno essere riesaminati almeno con cadenza annuale attraverso *audit* periodici compiuti da soggetti indipendenti. La fase di rivalutazione è, infatti, necessaria per l'organizzazione del soggetto da certificare in modo tale da poter avere un quadro costantemente aggiornato della sicurezza del trattamento, per limitare eventuali rischi residui e per individuarne dei nuovi.

La terza sezione disciplina, infine, gli obblighi relativi ai responsabili del trattamento. I criteri preminenti risultano sicuramente quelli concernenti la verifica del rapporto tra il responsabile e il titolare del trattamento o il *sub*-responsabile del trattamento. Verso entrambe le parti deve essere stipulato un contratto o un altro atto scritto vincolante ai sensi del diritto dell'unione che specifichi, l'oggetto e la durata del trattamento nell'ambito della domanda, la natura e le finalità di tale trattamento, la natura dei dati personali e le categorie di soggetti interessati, nonché gli obblighi e i diritti del responsabile del trattamento e del titolare o del sub-responsabile del trattamento, quale che sia l'altra parte. Rispetto agli altri criteri, quali quelli relativi alla sicurezza, all'analisi dei rischi o al trasferimento dei dati personali, la sezione fa riferimento ai criteri stabiliti nelle precedenti pagine del documento.

Con riguardo alla procedura di certificazione, la documentazione attualmente disponibile si focalizza principalmente sulla definizione dei criteri di certificazione, rispetto alla definizione della procedura in sé. Nonostante ciò, è possibile individuare sommariamente la procedura in cinque fasi:

1. la prima è la fase di autovalutazione dell'organismo richiedente la certificazione, il quale dovrà conformarsi ai criteri di certificazione GDPR-CARPA per poter, poi, procedere alla candidatura per la stessa;
2. nella seconda fase, viene valutata la domanda di certificazione e in caso positivo viene stipulato l'accordo di certificazione disciplinante gli obblighi tra l'OdC e il

[80] Cfr. CNPD, *GDPR-CARPA Certification Criteria*, *op. cit.*, 39-46; CNPD, *Schema illustrativo GDPR-CAPRA*, *op. cit.*, 20-22; J.T. HELMKE, H. LINK, H.H. SCHILD, *Zertifizierungskriterien für Verarbeitungstätigkeiten*, *op. cit.*, 105.

richiedente. La necessità di valutare le domande di certificazione è data per assicurarsi che il trattamento individuato dal richiedente rientri nell'oggetto e sia allineato con i criteri di certificazione;

3. successivamente saranno svolti gli *audit* di certificazione dall'ente di certificazione in base alla norma ISAE 3000 e ai criteri di certificazione. La metodologia di valutazione può comportare procedure variegate tra ispezione, osservazione, conferme, la ripetizione di *audit* o indagine, accessi o una combinazione tra di esse;
4. nella quarta fase viene presa la decisione di certificare l'organizzazione richiedente in base ad un *report* di valutazione redatto nella precedente fase e, in caso di giudizio positiva, la decisione viene comunicata al CNPD. Il certificato viene rilasciato dall'ente di certificazione per tre anni;
5. infine, nella quinta fase, viene monitorato il rispetto dei criteri GDPR-CARPA sulla base di *audit* annuali dell'OdC[81].

Per quanto riguarda gli Organismi di Certificazione che intendano rilasciare la certificazione GDPR-CARPA, questi dovranno ovviamente ottenere l'accreditamento. L'accreditamento per la certificazione GDPR-CARPA è gestito direttamente dal CNPD, richiedendo il rispetto dei requisiti previsti nell'art. 43 GDPR, del Regolamento (CE) n. 765/2008 e dei requisiti di accreditamento supplementari definiti dall'autorità di protezione dei dati lussemburghese[82]. Questi ultimi, in particolare, si basano sulle certificazioni ISAE 3000 (*audit*)[83], ISCQ1 (controllo di qualità delle organizzazioni di audit) e ISO/IEC 17065 (enti di certificazione). Gli OdC che possono essere accreditati sono esclusivamente quelli stabiliti in Lussemburgo, e il procedimento di accreditamento consta di un'analisi preliminare compiuta del CNPD, finalizzata a verificare il livello di competenza dell'ente, e da verifica completa da parte di esperti esterni. Conclusasi

[81] Cfr. O. REISCH, D. ALEXANDRE, G. DALLY, S. DEHMECHE, *CNPD adopts GDPR-CARPA certification criteria*, in *DLA PIPER – publications*, 2022, in Rete: *https://www.dlapiper.com/ en/insights/publications/2022/06/cnpd-adopts-gdpr-carpa-certification-criteria*; EY, *GDPR - CARPA certification with EY Luxembourg*, in Rete: *https://assets.ey.com/content/dam/ey-sites/ey-com/en_lu//topics/consulting/ey-luxembourg-gdpr-compliance-carpa-certification.pdf*. Le principali indicazioni sul processo e sulla metodologia di certificazione vengono attualmente fornite dall'OdC Grant Thornton A.A. rispetto ai procedimenti di certificazione gestiti dallo stesso. Per approfondire v. GRANT THORNTON AUDIT AND ASSURANCE S.A., *GDPR-CARPA Evaluation approach*, in Rete: *https://www.grantthornton.lu/en/services/audit-and-assurance/gdpr-carpa-certification/gdpr-carpa-certification-process/GDPR-CARPA-evaluation-approach/*.

[82] Cfr. CNPD, *Décision N° 8/2020 du 3 avril 2020 de la Commission nationale pour la protection des données portant approbation des critères d'agrément des organismes de certification*, 2020, in Rete: *https://cnpd.public.lu/content/dam/cnpd/fr/decisions-avis/2020/08-2020-Approbation-criteres-d-agrement-organismes-de-certification-signe.pdf*. I criteri di accreditamento aggiuntivi sono stati valutati anche dall'EDPB. Per approfondire, v. EDPB, *Parere 5/2020 sul progetto di decisione dell'autorità di controllo del Lussemburgo relativo all'approvazione dei requisiti per l'accreditamento di un organismo di certificazione ai sensi dell'articolo 43, paragrafo 3 (RGPD)*, 2020, in Rete: *https://edpb.europa.eu/sites/default/files/files/file1/edpb_opinion_202005_lu_requirementscertificationbodies_it.pdf*.

[83] ISAE 3000, è lo standard internazionale utilizzato per la verifica delle informazioni non-finanziarie. Per approfondire v. R. SIMNETT, *Assurance of sustainability reports Revision of ISAE 3000 and associated research opportunities*, in *Sustainability Accounting, Management and Policy Journal*, V. 3, N. 1, 2012, 89-98, in Rete: *https://doi.org/10.1108/20408021211223570*.

positivamente le verifiche, il CNPD rilascerà l'accreditamento all'OdC, il quale avrà una validità pari a cinque anni, con possibilità di rinnovo mediante un *audit* di rinnovo[84].

Infine, la certificazione lussemburghese è stata anche oggetto di diverse critiche. Come si è avuto modo di evidenziare precedentemente, la principale critica è stata rivolta al possibile conflitto di interessi del CNPD tra il proprio ruolo di autorità di controllo della protezione dei dati personali e quello di attore coinvolto nel processo di certificazione. Tale censura è stata però disinnescata dall'attribuzione di ogni potere di verifica e di attribuzione della certificazione ai soli OdC.

Altra critica riscontrata concernerebbe l'eccessiva onerosità della certificazione. Le misure tecniche ed organizzative incluse nei criteri di certificazione, infatti, richiederebbero ampie risorse finanziarie e umane da parte delle organizzazioni che intendono certificarsi. Il fatto che i requisiti siano progettati richiedendo un altro grado di documentazione delle procedure e misure di *accountability*, nonché la costante revisione delle stesse, provocherebbe l'adesione al meccanismo di certificazione solo delle imprese ed organizzazioni più grandi che hanno a disposizione tali risorse. Ciò, in pratica, potrebbe ridurre il numero di destinatari per la certificazione escludendo, potenzialmente, le micro, piccole e medie imprese in violazione dell'art. 42 par. 1 GDPR[85].

4.1 L'intervento dell'EDPB: Opinion 1/2022 sullo schema di decisione dell'Autorità di Supervisione del Lussemburgo riguardante i criteri di certificazione GDPR – CARPA

Come sempre, l'intervento del Comitato, ai sensi dell'art. 64 GDPR, mira a garantire la coerenza e la corretta applicazione dei criteri di certificazione tra le diverse autorità di controllo nell'UE. A tal fine, con il parere 1/2022 del 1° febbraio 2022, l'EDPB si è per la prima volta espresso rispetto ad un progetto di criteri di certificazione. L'azione del *Board* è stata sempre quella di indicare una serie di modifiche al progetto dei criteri ritenute necessarie per assicurare un'applicazione coerente del Regolamento.

I rilievi sollevati dal Comitato hanno riguardato tutte le sezioni dei criteri GDPR-CARPA, nonché l'impostazione metodologica adottata. Infatti, già rispetto alla determinazione del ToE, l'EDPB ha considerato insufficienti i relativi principi, raccomandando la specificazione ulteriore delle informazioni e dei criteri necessari per individuare il ToE[86]. Oltre ciò, è stata contestata la mancanza di chiarezza e analiticità di diversi criteri di certificazione rispetto a che cosa debba essere verificato e chi deve compiere il controllo. Ciò in ragione del fatto che, come si è visto, la certificazione GDPR-CARPA prevede una fase di *self-assessment* del richiedente, preliminare al

[84] Cfr. CNPD, *Procédure de la Commission nationale pour la protection des données (CNPD) relative à l'agrément des organismes de certification*, 2021, 7, in Rete: *https://cnpd.public.lu/content/dam/cnpd/fr/professionnels/certification/Procedure-relative-a-l-agrement-des-organismes-de-certification.pdf*.

[85] Cfr. J.T. HELMKE, H. LINK, H.H. SCHILD, *Zertifizierungskriterien für Verarbeitungstätigkeiten*. In *Datenschutz Datensich*, *op. cit.*, 107. Per approfondire, inoltre, v. E. KOULIERAKIS, *Certification as Guidance for Data Protection by Design*, 2023, 14-15, in Rete: *https://dx.doi.org/10.2139/ssrn.4330542*.

[86] Cfr. EDPB, *Opinion 1/2022 on the draft decision of the Luxembourg Supervisory Authority regarding the GDPR – CARPA certification criteria*, 2022, in Rete: *https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-12022-draft-decision-luxembourg_en*.

procedimento di verifica condotto dall'OdC e necessario per adeguare la propria organizzazione ai requisiti della certificazione. Ebbene, rispetto a tale fase, il comitato osserva come nei criteri di certificazione non sempre siano definiti gli elementi su come l'autovalutazione dovrebbe essere effettuata dal richiedente; con la criticità che il soggetto che intende certificarsi, non essendo in grado di comprendere lucidamente gli obblighi tecnici ed organizzativi (soprattutto documentali) richiesti nella fase di *self-assessment* per accedere alla certificazione, questi non sarà nemmeno in grado di prevedere quali valutazioni saranno poi condotte dall'OdC. Questa incertezza viene particolarmente riscontrata dal *Board* nei criteri relativi ai principi del trattamento e, nello specifico, nell'individuazione della base giuridica per il trattamento. Pertanto, il Comitato ha raccomandato al CNPD di fornire ulteriori elementi che dovranno essere presi in considerazione dal richiedente nello svolgimento delle autovalutazioni, in modo da chiarire anche ciò che sarà controllato dall'organismo di certificazione[87].

Inoltre, sempre con riferimento alla verifica di una base giuridica valida del trattamento, l'EDPB ha precisato come l'analisi della validità, correttezza e applicabilità di una base giuridica dipenda dalla natura, portata, contesto e finalità del trattamento, rendendosi necessario specificare tali componenti anche nei criteri di certificazione[88].

In generale il Comitato ha riscontrato diverse carenze di concretezza, sufficienza ed esaustività dei criteri, tali da non poter permettere agli OdC di compiere un'analisi corretta delle misure implementate dal soggetto che intende certificarsi a garanzia dei diritti degli interessati. Per tale ragione è stato raccomandato al CNPD di modificare i criteri in modo da consentire un'oggettiva ed esaustiva valutazione dell'OdC[89].

Rispetto agli obblighi applicabili ai titolari del trattamento l'EDPB non riscontra importanti criticità, se non diverse osservazioni rispetto al rapporto tra il DPO e il titolare del trattamento. In relazione al rapporto tra il titolare e il responsabile del trattamento vengono compiute alcune osservazioni sul contratto *ex* art. 28 GDPR per la protezione dei dati e, nello specifico, sui contenuti che questo deve avere[90].

Con riguardo ai criteri relativi al responsabile del trattamento, il *Board* ha invitato il CNPD ad inserire dei criteri specificamente rivolti ai *sub*-responsabili del trattamento e ai rispettivi obblighi di assistenza e collaborazione con il responsabile e il titolare del trattamento.

Infine, ulteriori precisazioni vengono richieste in relazione ai criteri di valutazione delle modalità di gestione delle istanze degli interessati e alla sottosezione relativa all'analisi del rischio determinato dal trattamento, necessitandosi, in quest'ultimo caso,

[87] Cfr. *ivi*, 7-8.

[88] Il *Board* ha ulteriormente riscontrato delle lacune anche con riferimento ai criteri relativi al consenso per il trattamento, evidenziando come debbano essere inseriti dei criteri di verifica affinché il consenso acquisito per il trattamento da certificare si possa considerare informato e inequivocabile. Cfr. *ivi*, 8-9.

[89] Cfr. *ivi*, 10.

[90] Cfr. *ivi*, 11-12. In particolare, il Comitato ha ritenuto di dover precisare che il DPO, benché abbia un ruolo significativo nell'attività di monitoraggio della conformità al GDPR delle attività di trattamento, non può essere considerato il soggetto responsabile nel valutare l'attuazione delle misure volte a garantire tale conformità.

precisazioni in ordine ai possibili tipi di rischio riscontrabili, alle misure tecniche ed organizzative implementabili e alla metodologia di verifica di queste ultime[91].

Come anticipato, la valutazione iniziale dell'EDPB sui criteri GDPR-CARPA è stata insufficiente, in quanto presenterebbe il rischio di determinare un'inconsistente applicazione del GDPR. Tutti i rilievi sollevati dal Comitato sono comunque stati corretti e inseriti nella versione definitiva dello schema di certificazione [92]. Pertanto, nell'immediato futuro si potrà vedere come verrà percepita dalla prassi l'applicazione della certificazione GDPR-CARPA, atteso che, al momento della stesura di questo elaborato, sono già stati accreditati diversi Organismi di Certificazione[93].

5 EUROPRIVACY©: Il Parere 28/2022 segna la nascita del primo Sigillo europeo per la protezione dei dati

Il 10 ottobre con Parere 28/2022 reso ai sensi dell'art. 64, par. 2 e dell'art. 42, par. 5 del GDPR, l'EDPB si è pronunciato sui criteri di certificazione Europrivacy© presentati dall'Autorità di controllo del Lussemburgo come certificazione comune europea. La certificazione è stata sviluppata dal Centro europeo per la certificazione e la privacy (ECCP) con la cooperazione di numerosi esperti nel settore della protezione dei dati personali e, attraverso l'approvazione da parte del Comitato, rappresenta il primo Sigillo europeo per la protezione dei dati con validità in tutti gli Stati membri dell'UE[94].

Il meccanismo di certificazione Europrivacy© è uno schema generico capace di contemplare un'ampia gamma di trattamenti di dati personali eseguiti in settori eterogenei. Possono aderire alla certificazione sia titolari che responsabili del trattamento stabiliti nell'Unione europea, al fine di dimostrare la propria conformità al GDPR. Lo scopo della certificazione è quello di rendere la protezione dei dati personali maggiormente effettiva ed efficacie, trasformandolo da mero adempimento ad un *asset* spendibile nel mercato. La finalità, infatti, rimane sempre quella di accrescere la fiducia degli interessati (e in generale degli *stakeholders*) nelle nuove tecnologie e nelle imprese che le offrono, permettendo di identificare chiaramente e selezionare le organizzazioni che fanno della *data protection* la propria strategia di *business*, traducendosi in un vantaggio competitivo.

Al livello del titolare o del responsabile del trattamento, invece, la certificazione permetterebbe di identificare correttamente le potenziali lacune e criticità in relazione agli adempimenti previsti per la protezione dei dati personali, riducendo i rischi legali,

[91] Cfr. *ivi*, 13-15. In particolare, il *Board* incoraggia la CNPD a chiarire che esistono processi per misurare e garantire l'efficacia di detto piano, in modo da garantire che i criteri di certificazione siano auto esplicativi e che l'organismo di certificazione possa sapere cosa deve verificare dalla sola formulazione dei criteri.

[92] Come indicato dalla CNPD nei criteri di certificazione approvati: "*Considérant qu'en date du 1er février 2022, le CEPD a adopté un avis relatif au projet de décision sur les critères de certification GDPR-CARPA lui soumis par la CNPD. Une mise à jour de son projet de décision, qui a pris en compte toutes les recommandations et tous les encouragements de l'avis précité du CEPD, a été soumis par la CNPD au CEPD le 22 février 2022*". Cfr. CNPD, *GDPR-CARPA Certification Criteria*, *op. cit.*, 1.

[93] Ossia la EY PFS Solutions Luxembourg e la Grant Thornton Audit and Assurance S.A., Luxembourg.

[94] La certificazione Europrivacy© è, infatti, stata sviluppata da un gruppo di ricercatori, professionisti ed esperti del settore *data protection* sotto il programma di ricerca europeo Horizon 2020. Cfr. EUROPRIVACY *website*, in Rete: *https://www.europrivacy.org/*.

finanziari e reputazionali conseguenti a possibili sanzioni delle autorità di controllo[95]. La certificazione Europrivacy©, infatti, può essere usata per: verificare la conformità delle attività di trattamento dei dati personali; selezionare i possibili responsabili del trattamento valutandone la professionalità mediante il sigillo di certificazione; verificare l'adeguatezza delle misure implementate per i trasferimenti transfrontalieri di dati, appurando, eventualmente, la conformità delle terze parti interessate; assicurare il rispetto e il pieno esercizio dei diritti degli interessati.

Tali valutazioni sono possibili mediante i 'criteri fondamentali' della certificazione, i quali si occupano di verificare e controllare l'adeguatezza delle misure tecniche ed organizzative poste in essere per garantire la conformità del trattamento al Regolamento[96]. Con la certificazione Europrivacy© possono essere inclusi nel ToE anche quei trattamenti soggetti a contitolarità. In tale ipotesi, tuttavia, l'OdC dovrà svolgere un'analisi approfondita in merito agli adempimenti reciprocamente stabiliti dai diversi contitolari del trattamento: potranno essere sottoposti a certificazione solamente i trattamenti per i quali il singolo contitolare del trattamento, richiedente la certificazione, sia pienamente responsabile della sua conformità[97].

Oltre ai requisiti di carattere generale, lo schema include altresì criteri specifici che renderebbero la certificazione modulabile e applicabile a taluni specifici trattamenti o settori di attività. Ciò permetterebbe di ricomprendere nel ToE della certificazione anche trattamenti facenti parte di tecnologie emergenti e innovative come AI, IoT, blockchain, *smart cities*, *eHealth*. Nel parere, l'EDPB ha accolto con favore l'inclusione di criteri specifici in grado di consentirne la scalabilità e l'applicabilità rispetto a specifici trattamenti o settori di attività[98]. Inoltre, il fatto che la certificazione preveda sia criteri di carattere generale che specifici permetterebbe non solo alle grandi organizzazioni di aderire allo schema Europrivacy©, ma anche le micro, piccole e medie imprese[99].

---

[95] Cfr. PR NEWSWIRE, *European Centre for Certification and Privacy: Europrivacy - The GDPR European Data Protection Seal Approved by the EU, a New Era for Privacy and Data Protection Compliance*, 12 ottobre 2022, in Rete: *https://www.prnewswire.com/news-releases/european-centre-for-certification-and-privacy--europrivacy--the-gdpr-european-data-protection-seal-approved-by-the-eu-a-new-era-for-privacy-and-data-protection-compliance-301647958.html*.

[96] Cfr. EDPB, *Parere 28/2022 sull' approvazione dei criteri di certificazione Europrivacy da parte del Comitato come sigillo europeo per la protezione dei dati a norma dell'articolo 42, paragrafo 5, del regolamento generale sulla protezione dei dati (RGPD)*, 2022, 4, in Rete:*https://edpb.europa.eu/system/files/2023-03/edpb_opinion_202228_europrivacy_eu_data_protection_seal_it.pdf*.

[97] Cfr. *ivi*, 5; LIEDEKERKE, *The European Data Protection Seal as a certification tool*, 2023, in Rete: *https://liedekerke.com/en/insights/the-european-data-protection-seal-as-a-certification-tool*. Di conseguenza, come anche precisato dal *Board* nel parere: "*l'accordo concluso tra il richiedente e gli altri contitolari del trattamento coinvolti nel ToE per quanto riguarda le rispettive responsabilità per l'osservanza degli obblighi di cui al GDPR potrebbe, a seconda del contesto e della natura del trattamento, impedire al richiedente di soddisfare i criteri di certificazione*".

[98] Cfr. EDPB, *Parere 28/2022 sull' approvazione dei criteri di certificazione Europrivacy*, *op. cit.*, 4. Il Comitato ha comunque precisato che i criteri relativi a criteri specifici non sono oggetto del parere per l'approvazione della certificazione quale Sigillo Europeo.

[99] Non ci sono limiti dimensionali per l'ammissione della domanda di certificazione di un ente, ma, ovviamente, le grandi imprese saranno quelle più interessate, in quanto, necessitano di un meccanismo celere per dimostrare la conformità. Anche entità pubbliche: ospedali, università, centri di ricerca. Come evidenziato dal direttore del ECCP Sébastien Ziegler: "*l'ambizione era quella di ottenere uno schema inclusivo, adatto a tutti sia in termini soggettivi (pubblico-privato, piccolo-grande), che in termini oggettivi*

Essendo approvata quale Sigillo europeo per la protezione dei dati personali, la certificazione Europrivacy© può aiutare titolari e responsabili del trattamento a adottare una strategia di *compliance* valida in tutti gli Stati membri. Ciò in ragione del fatto che, come si è avuto modo di descrivere nel Capitolo II, i criteri di certificazione, per essere approvati a livello europeo, devono prendere in considerazione tutte le legislazioni nazionali degli Stati membri, oltre che alle sentenze della CGUE e alla prassi dell'EDPB.

È comunque da sottolineare che il meccanismo di certificazione Europrivacy© non è una certificazione ai sensi dell'art. 46, par. 2, lett. f) del GDPR per i trasferimenti internazionali di dati personali. Pertanto, esso non fornisce garanzie adeguate nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali, il quale potrà avvenire solamente al rispetto dei principi contenuti nel Capo V del Regolamento[100].

Ulteriore nota positiva della certificazione è rappresentata dal fatto che i suoi criteri possono essere integrati con ulteriori norme tecniche e prassi esistenti nel settore della protezione delle informazioni e dei dati. Infatti, Europrivacy© sfrutta entrambe le certificazioni ISO/IEC 17065, per la certificazione di processi, prodotti e servizi, e ISO/IEC 17021-1, per la certificazione di processi di gestione, al fine di renderla applicabile a vasti contesti e ad un ampio insieme di attività di elaborazione dei dati e delle informazioni. Tale duplice allineamento ad entrambe le certificazioni ISO permette potenzialmente di combinare la certificazione Europrivacy©, rilasciata ai sensi del GDPR; con altre certificazioni attestanti la sicurezza dei sistemi di gestione delle informazioni (e in particolare il modello ISO/IEC 27001 e ISO/IEC 27701)[101].

La metodologia della certificazione è quella di favorire la trasparenza degli adempimenti privacy riducendo al minimo le possibilità di interpretazione soggettiva degli obblighi del GDPR. Proprio la scarsa chiarezza, infatti, determina la disomogenea applicazione dei principi della protezione dei dati personali da parte dei titolari e responsabili del trattamento; perciò, attraverso l'individuazione di criteri oggettivi per la valutazione della conformità si potrà garantire l'applicazione coerente del GDPR[102].

I criteri fondamentali di Europrivacy© consentono di valutare la corrispondenza del trattamento rispetto a tutti gli elementi rilevanti per la protezione dei dati personali. In particolare, i criteri analizzano:

(rispetto al tipo di trattamento da valutare), rendendo omogeneo ogni processo di conformità". Cfr. S. ZIEGLER, intervento presentato al seminario *Il meccanismo delle certificazioni con il GDPR – Il primo sigillo europeo per la protezione dei dati: la certificazione di Europrivacy*, *op. cit*.

[100] Cfr. EDPB, *Parere 28/2022 sull' approvazione dei criteri di certificazione Europrivacy*, *op. cit.*, 4.

[101] Cfr. COMMISSIONE EUROPEA, *Europrivacy: the first certification mechanism to ensure compliance with GDPR*, 2022, in Rete: *https://digital-strategy.ec.europa.eu/en/news/europrivacy-first-certification-mechanism-ensure-compliance-gdpr*.

[102] In particolare, per la certificazione Europrivacy© tutti i criteri sono stati sviluppati e vengono aggiornati dal Centro Europeo per la Certificazione e la Privacy (ECCP) e dal suo Europrivacy© *International Board of Experts*.

- la liceità del trattamento per ogni singola operazione rientrante nel ToE. Il soggetto da certificare dovrà dimostrare di rispettare ogni condizione richiesta per le diverse basi giuridiche del trattamento[103];
- la corretta attuazione dei principi del trattamento. L'ente che intende certificarsi dovrà, quindi, dimostrare che i dati personali trattati siano adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per le quali sono trattati[104];
- che il trattamento di categorie particolari di dati personali, sia lecitamente compiuto sulla base di una base giuridica, constatando il rispetto delle misure previste per il trattamento. Inoltre, i criteri richiedendo, da parte del DPO dell'organizzazione, un'analisi dei rischi per i diritti e libertà degli interessati derivanti dal medesimo trattamento[105];
- che siano attuate misure per la gestione dei diritti degli interessati, fornendo a questi ultimi un'informativa adeguata e garantendo un agevole esercizio dei diritti di rettifica, cancellazione (diritto all'oblio), limitazione del trattamento, portabilità e diritto di opposizione[106];
- che gli obblighi del titolare o del responsabile del trattamento, quali, ad esempio, il Registro dei trattamenti, la nomina del DPO, la valutazione dei rischi (mediante la DPIA) e la predisposizione di policies siano correttamente eseguiti. I criteri compiono anche un'approfondita valutazione sugli accordi contrattuali tra titolare e responsabile del trattamento in modo che questi siano in linea con l'art. 28 GDPR[107];
- la corretta attuazione dei principi della DPbDD e della minimizzazione dei dati, nonché l'adozione di misure tecniche e organizzative che garantiscano la riservatezza, l'integrità e la disponibilità dei dati, nonché la previsione di procedure finalizzate a garantire il corretto e tempestivo adempimento degli obblighi di notifica dei *data breach*[108];
- l'individuazione di tutti i trasferimenti di dati verso paesi terzi che siano coinvolti nel trattamento rientrante nel ToE. In particolare, il soggetto che richiede la certificazione dovrà premunirsi di tutta la documentazione necessaria ad illustrare le misure e le garanzie poste in essere, in conformità con il Capo V del GDPR, per assicurare un livello di protezione dei dati adeguato a quello europeo[109].

Infine, per conseguire il Sigillo europeo Europrivacy©, l'organismo richiedente la certificazione, nell'adeguamento della propria organizzazione ai criteri di certificazione, dovrà tener conto della legislazione nazionale in materia di protezione dei dati personali

[103] Cfr. ECCP, *Europrivacy GDPR Core Criteria*, 2020, 1-3, in Rete: *https://community .europrivacy.com/ europrivacy-gdpr-core-criteria/*.
[104] Cfr. EDPB, *Parere 28/2022 sull' approvazione dei criteri di certificazione Europrivacy*, *op. cit.*, 5-6.
[105] Cfr. ECCP, *Europrivacy GDPR Core Criteria*, *op. cit.*, 4-5.
[106] Cfr. *ivi*, *5*-12.
[107] Cfr. EDPB, *Parere 28/2022 sull' approvazione dei criteri di certificazione Europrivacy*, *op. cit.*, 6; ECCP, *Europrivacy GDPR Core Criteria*, *op. cit.*, 13-16. La particolarità rispetto alle altre certificazioni è che i criteri prevedono che il titolare o il responsabile del trattamento debbano designare un responsabile della protezione dei dati anche nel caso in cui questi ultimi non siano tenuti a nominarlo ai sensi dell'art. 37 GDPR.
[108] Cfr. ECCP, *Europrivacy GDPR Core Criteria*, *op. cit.*, 16-19.
[109] Cfr. *ivi*, 22-24.

di tutti gli Stati membri. Stando a quanto indicato nello schema dei criteri di certificazione, il richiedente dovrà redigere una relazione particolareggiata necessaria a dar conto delle misure adottate per rendere il trattamento oggetto di valutazione conforme alle varie normative nazionali e delle iniziative correttive eventualmente intraprese ove non tutti i requisiti nazionali siano stati soddisfatti[110].

Purtroppo, la documentazione attualmente a disposizione non permette di indagare in profondità il procedimento di certificazione che i titolari e i responsabili dovranno seguire. D'altronde sia i criteri di certificazione pubblicati che il parere dell'EDPB si concentrano esclusivamente sui principi e i controlli del Sigillo europeo Europrivacy©. Ciononostante, si può sommariamente descrivere il processo di certificazione in tre principali fasi:

1. fase preparatoria, ove il rispetto dei criteri di certificazione generali e nazionali deve essere documentato dal richiedente e presentato all'OdC;
2. fase di certificazione, in cui il rispetto dei criteri di certificazione è certificato da un OdC accreditato dall'ECCP, che, se accerta positivamente la conformità, assegna il sigillo di certificazione di durata triennale;
3. fase di monitoraggio, nella quale il rispetto dei criteri Europrivacy© deve essere mantenuto e monitorato, anche mediante *audit* di sorveglianza annuali.[111]

In conclusione, come d'altronde già osservato dall'EDPB, i criteri di certificazione Europrivacy© permetterebbero un'applicazione uniforme e coerente del GDPR all'interno dei paesi membri dell'Unione. Questo risultato, tuttavia, non ritenuto totalmente soddisfacente. Il BfDI, l'Autorità federale tedesca per la protezione dei dati personali, ha criticato l'approvazione dei criteri ritenendo che, nonostante questi fossero in linea con il GDPR, mancassero di precisione e chiarezza nell'implementazione, rendendo difficoltosa l'applicazione uniforme dei criteri[112]. La prevalenza di controlli di un taglio prevalentemente giuridico, a discapito della previsione di criteri tecnici precisi, causerebbe infatti l'indeterminatezza dello schema di certificazione, la cui concreta applicazione rischierebbe di essere rimessa all'interpretazione dei diversi OdC accreditati al rilascio della stessa.

Resta il fatto che l'attuazione del primo Sigillo europeo per la protezione dei dati personali rappresenta uno sviluppo importante nell'applicazione del GDPR, in quanto coadiuverebbe le istituzioni europee nella formazione e nello sviluppo di una cultura rafforzata della *data protection*. Solo in questo modo si raggiungerebbe lo scopo del GDPR, ossia garantire la tutela e la garanzia dei diritti e delle libertà fondamentali degli individui-interessati dal trattamento, permettendo, altresì la libera circolazione dei dati

[110] Cfr. *ivi*, 2. Rispetto ai criteri aggiuntivi per il Sigillo europeo, l'ECCP mette a disposizione del soggetto che intende certificarsi e dell'esperto che si occuperà delle valutazioni una lista degli obblighi normativi imposti dai vari Paesi membri dell'Unione.

[111] Cfr. ECCP, *Europrivacy Overview*, in Rete: *https://www.europrivacy.org/en/ep/overview*; G. SOMERS, P. GRYFFROY, *The first EU-wide GDPR Certification Scheme – Europrivacy (Tm/®) explained in 5 questions*, in *Timelex*, 2022, in Rete: *https://www.timelex.eu/en/europrivacy*.

[112] Cfr. BFDI, *The 2022 Activity Report of the Federal Commissioner for Data Protection and Freedom of Information*, *op. cit.*, 78.

personali per permettere la fisiologica evoluzione del mercato unico europeo in un mercato unico digitale basato sui dati[113].

[113] Proprio a fronte della novità dello strumento nel mercato europeo si segnala che anche Accredia ha provveduto a notificare all'EDPB una lettera con diversi dubbi e questioni relativi al Sigillo Europeo per la Protezione dei dati personali, nonché alla certificazione Europrivacy©. Alle diverse questioni poste dall'organismo nazionale di accreditamento italiano il Comitato ha provveduto a rispondere con la Lettera ad Accredia dd. 01.08.2023, pubblicata in Rete: *https://edpb.europa.eu/system/files/2023-08/edpb_letter_out2023-0061_replytoaccredia_en.pdf*.

CAPITOLO IV - LE CERTIFICAZIONI GDPR NELLA STRATEGIA DIGITALE DELL'UNIONE EUROPEA

1 Introduzione: il futuro europeo definito dalla European Data Strategy, Digital Services Package e dalla regolazione dell'intelligenza artificiale

I dati personali sono al centro della trasformazione digitale della società e dell'economia in tutti i settori di attività. Il volume dei dati prodotti a livello mondiale è, infatti, in rapida crescita, dai 33 *zettabyte* del 2018 ai 175 *zettabyte* previsti nel 2025. Per tale ragione la Commissione europea ha intrapreso a partire dal 2020 la "Strategia dei dati"[1]. Se attualmente un numero ridotto di imprese tecnologiche non-europee detiene la maggior parte dei dati, personali e non personali, disponibili, lo scenario nell'Unione dovrebbe cambiare nel prossimo futuro. L'obiettivo, appunto, è quello di creare uno "spazio unico europeo di dati" o un "mercato unico di dati" nel quale nel quale i dati personali e non personali possano circolare e i servizi digitali proliferare in un quadro giuridico sicuro che garantisca lo sviluppo dell'economia digitale europea[2].

Su questo fronte la Commissione ha già intrapreso diverse iniziative a partire dal 2014, di cui il GDPR ne è il più importante esempio. Quest'ultimo rappresenta la base di partenza affinché si possa istituire un quadro giuridico ed economico solido per la fiducia nei servizi digitale. Già il Regolamento sulla protezione dei dati personali, all'art. 1, dopo aver precisato che il suo scopo è proteggere i diritti e le libertà fondamentali degli individui, con particolare riferimento alla protezione dei dati personali, chiarisce che "*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*" [3]. La circolazione dei dati personali rappresenta la nuova fonte e il presupposto necessario per lo sviluppo del Mercato Unico Digitale.

Ecco che, quindi, dopo un primo periodo di tempo in cui è stata rafforzata la tutela dei dati personali verso gli interessati, apparentemente prevedendo una serie di requisiti da osservare per la loro circolazione, ora si assiste ad una progressiva apertura mercé la presentazione di un pacchetto legislativo volto – almeno a livello di declamazioni - a garantire la circolazione, l'accesso e lo sfruttamento di dati personali e non personali da parte delle imprese e degli organismi di ricerca per dar spinta all'innovazione nel Mercato Unico europeo.

Oltre al condivisibile obiettivo della circolazione dei dati, la Commissione ha intrapreso un ulteriore strategia necessaria per la creazione di uno spazio neutrale nel quale il diritto dell'UE possa essere applicato con efficacia a tutti i prodotti e i servizi digitali basati sui dati. Con il "Pacchetto sui servizi digitali", è stato intrapreso un percorso che permetterà di creare uno spazio digitale più sicuro in cui siano tutelati i

[1] Cfr. COMMISSIONE EUROPEA, *COM/2020/66, "Una strategia europea per i dati",* 2020, in Rete: *https://eur-lex.europa.eu/legal-content/it/txt/?uri=celex%3a52020dc0066*.
[2] Cfr. *ivi*, 5-6.
[3] Per approfondire v. M.L. MONTAGNANI, *La libera circolazione dei dati al bivio. Tra tutela dei dati personali e promozione dell'Intelligenza artificiale europea*, in *Mercato Concorrenza Regole*, 2/2019, 293 ss.

diritti fondamentali di tutti gli utenti dei servizi digitali nonché delle condizioni di parità per promuovere l'innovazione, la crescita e la competitività, sia nel mercato unico europeo che a livello globale[4].

A fronte di ciò, dal novembre 2020 la Commissione europea ha avanzato molteplici iniziative legislative nell'ambito della Strategie europee dei dati e dei servizi digitali, in particolare la legge sui servizi digitali (DSA), la legge sui mercati digitali (DMA), la legge sulla *governance* dei dati (DGA), il regolamento sull'intelligenza artificiale (AIA) e una quinta proposta relativa all'accesso e all'uso dei dati (DA). Ciascuna di queste proposte mira a mirano a facilitare l'ulteriore utilizzo e condivisione dei dati (personali) tra un maggior numero di soggetti pubblici e privati all'interno dell'economia dei dati, a sostenere l'uso di tecnologie specifiche come i *big data* e l'IA e a regolamentare le piattaforme online e i *gatekeeper*.

Ogniuna di queste ha un punto in comune fondamentale, ossia i dati. Di conseguenza, i citati interventi legislativi pongono le proprie basi sul GDPR e sulle garanzie e gli obblighi previsti da quest'ultimo. Tutti questi provvedimenti influenzano, in un modo o nell'altro, la protezione dei dati personali, incidendo sui diritti e sulle libertà degli interessati. La *data protection* rappresenta il requisito fondante di tutte le norme della strategia economica digitale, risultando non solo necessaria, ma imprescindibile nel contesto economico-giuridico europeo. Il fatto che il GDPR abbia un ruolo più o meno importante in ciascuna di questi interventi normativi determina altresì l'applicabilità delle sue previsioni, fra cui quelle delle certificazioni e codici di condotta. La strategia della co-regolamentazione, infatti, non è stata abbandonata dalla Commissione, ma, come si avrà modo di spiegare successivamente, questa è stata implementata in ognuna di queste proposte in modo più o meno diverso.

In via preliminare, è necessario offrire una breve panoramica dei nuovi interventi legislativi e sugli obblighi che pongono all'industria digitale:

- il Regolamento (UE) 2022/2065 sui servizi digitali (*Digital Services Act*) impone alle autorità competenti di vigilare sui sistemi di raccomandazione di piattaforme online molto grandi (che spesso comportano la profilazione degli interessati ai sensi del GDPR); nonché le misure adottate per valutare e mitigare i rischi sistemici, compreso il rischio per il diritto alla vita privata[5];
- il Regolamento (UE) 2022/1925 sui mercati digitali (*Digital Market* Act) impone ai *gatekeeper* di agevolare l'esercizio della portabilità dei dati in linea con il GDPR e di fornire, a determinate condizioni, l'accesso ai dati, compresi i dati personali, ai sensi dell'articolo 6, par. 1, lett. h) e i), e ai dati resi anonimi ai sensi dell'articolo 6, par. 1, lett. j). Inoltre, vengono previsti ulteriori obblighi che intendono limitare le possibili condotte anticoncorrenziali dei *gatekeeper*[6];

[4] Cfr. CONSIGLIO EUROPEO, *Pacchetto sui servizi digitali,* 2022, in Rete: *https://www.consilium.europa.eu/it/policies/digital-services-package/*.

[5] Cfr. EUROPEAN COMMISSION, *The Digital Services Act package*, 2023, in Rete: *https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package*; *Id*, *Digital Services Act: Questions and Answers*, 2023, in Rete: *https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers*.

[6] Cfr. EUROPEAN COMMISSION, The Digital Markets Act, 2023, in Rete: *https://digital-markets-act.ec.europa.eu/index_en.*

- il Regolamento (UE) 2022/868 sulla governance europea dei dati (*Data Governance Act*) mira ad aumentare la fiducia nella condivisione dei dati, rafforzare i meccanismi per aumentare la disponibilità e superare gli ostacoli tecnici al riutilizzo dei dati. La finalità è quella di sviluppare il potenziale dei dati personali e non personali a vantaggio dei cittadini e delle imprese per sviluppare prodotti e servizi innovativi. Le misure previste dal regolamento concernono l'introduzione di meccanismi per facilitare il riutilizzo di determinati dati del settore pubblico, la previsione di misure volte a garantire che nuovi soggetti, ossia gli 'intermediari dei dati', fungano da organizzazioni affidabili della condivisione dei dati all'interno del mercato comune europeo e l'inserimento di misure volte a rendere più facile per le persone fisiche e le imprese mettere a disposizione i propri dati a beneficio della società[7];
- la proposta di Regolamento sui dati (*Data Act*) è invece rivolta a rimuovere gli ostacoli all'accesso ai dati sia per i soggetti privati che pubblici, sbloccando il valore dei dati generati dagli oggetti connessi all'*Internet of Things*, i quali rappresentano una delle aree di innovazione chiave nei prossimi decenni. Vengo quindi definite una serie di regole che consentiranno agli utenti dei dispositivi intelligenti di accedere ai dati generati da tali dispositivi per eventualmente condividerli con terzi. Viene inoltre incentivata una maggiore interoperabilità tra i servizi di trattamenti dei dati rafforzando il diritto alla portabilità a favore degli utenti interessati-persone fisiche e delle imprese[8];
- la proposta di Regolamento sull'intelligenza artificiale (*Artificial Intelligence Act*) stabilisce, invece, la prima proposta regolatoria al mondo per la creazione, sviluppo e commercializzazione dei sistemi di intelligenza artificiale. La proposta prevede un meccanismo di gestione dell'IA basata sul rischio, a seconda delle attività e degli usi a cui può essere assegnata. La norma prevede quindi diversi livelli di rischio a cui seguono delle differenti norme di *governance* dell'IA, sia nella fase iniziale di sviluppo che in quella finale di messa sul mercato e monitoraggio. Tale proposta è quella che incide maggiormente sul GDPR in quanto i dati personali, più dei dati non personali, sono quelli maggiormente necessari per lo sviluppo e l'evoluzione delle IA[9].

La complessità di questi nuovi interventi legislativi può causare ambiguità nell'applicazione uniforme della disciplina sulla protezione dei dati personali. Per questo motivo si rendono necessari la presenza di strumenti che possano migliorare la coerenza delle nuove proposte con il quadro esistente in materia di protezione dei dati al fine di garantirne l'effettiva attuazione. Specie per gli interventi che determineranno una maggiore apertura e condivisione dei dati personali, è necessario che si definiscano fin

[7] Cfr. EUROPEAN COMMISSION, *European Data Governance Act*, 2022, in Rete: *https://digital-strategy.ec.europa.eu/en/policies/data-governance-act*; *Id*, *Data Governance Act explained*, 2022, in Rete: *https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained*.

[8] Cfr. EUROPEAN COMMISSION; *Data Act*, 2023, in Rete: *https://digital-strategy.ec.europa.eu/en/policies/data-act*; *Id*, *Data Act – Questions and Answers*, 2023, in Rete: *https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_1114*.

[9] Cfr. PARLAMENTO EUROPEO, *Normativa sull'IA: la prima regolamentazione sull'intelligenza artificiale*, 2023, in Rete: *https://www.europarl.europa.eu/news/it/headlines/society/20230601STO93804/normativa-sull-ia-la-prima-regolamentazione-sull-intelligenza-artificiale*.

da subito garanzie idonee a assicurare un livello elevato di protezione dei dati personali, in ragione dei possibili pregiudizi che gli interessati potrebbero subire[10].

2 Digital Services Package: come il mercato dei servizi digitali può impattare sulla protezione dei dati personali

2.1 Digital Services Act

Lo scorso 16 novembre 2022 ha segnato l'entrata in vigore del Regolamento (UE) 2022/2065 sui servizi digitali (anche detto *Digital Services Act*, d'ora in avanti DSA), presentato dalla Commissione nel dicembre 2020 quale componente principale della nuova strategia del mercato unico digitale europeo[11].

Lo scopo dichiarato del DSA è contribuire al corretto funzionamento del mercato interno dei servizi della società dell'informazione, stabilendo norme armonizzate per un ambiente online sicuro, prevedibile e affidabile, che faciliti l'innovazione e in cui i diritti fondamentali sanciti dalla CDFUE, compreso il principio della protezione dei consumatori, siano tutelati in modo effettivo[12]. Per tali ragioni il Reg. (UE) 2022/2065 ridefinisce le norme applicabili alle piattaforme online in tema di gestione dei servizi digitali. Vengono introdotte nuove norme in materia di trasparenza, obblighi informativi e *accountability* per i prestatori di determinati "*servizi della società delle informazioni*", ovvero i soggetti che offrono servizi a distanza, per via elettronica, a richiesta di un destinatario, "*normalmente dietro retribuzione*"[13].

Gli obblighi e le responsabilità per gli *Internet Service Provider* sono distribuiti a seconda dei servizi che questi ultimi forniscono[14] , ma è evidente che un impatto

[10] Cfr. EDPB, *Statement on the Digital Services Package and Data Strategy*, 2021, in Rete: *https://edpb.europa.eu/system/files/2021-11/edpb_statement_on_the_digital_services_package_and_data_strategy_en.pdf*.

[11] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), in Rete: *https://eur-lex.europa.eu/legal-content/it/txt/pdf/?uri=celex:32022r2065*. Il regolamento avrà piena applicazione a partire dal 17 febbraio 2024.

[12] Cfr. art. 1, par. 1 DSA.

[13] In altri termini, il *Digital Services Act* riguarda tutti gli operatori del mercato digitale, dai social network alle piattaforme e-commerce e i motori di ricerca. Cfr. art. 1, par. 1, lett. b) Direttiva (UE) 2015/1535: "*«servizio»: qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi*".

[14] In generale, i servizi presi in considerazione dal DSA vengono suddivisi dall'art. 3, lett. g) in: 1. semplice trasporto: si ricomprendono i punti di interscambio internet, i punti di accesso senza fili, le reti private virtuali, i risolutori e i servizi di DNS, i registri dei nomi di dominio di primo livello, gli organismi di certificazione che rilasciano certificati digitali, il VOIP e altri servizi di comunicazione interpersonale; 2. memorizzazione temporanea: quei servizi intermediari che includono la sola fornitura di reti per la diffusione di contenuti, proxy inversi o proxy di adattamento dei contenuti. Sono quei servizi fondamentali per garantire una trasmissione fluida ed efficiente delle informazioni fornite su internet; 3. memorizzazione di informazioni: si tratta di quei servizi di hosting che includono categorie come la c.d. nuvola informatica, la memorizzazione di informazioni di siti web, i servizi di referenziazione a pagamento o i servizi che consentono la condivisione di informazioni e contenuti online, compresa la condivisione e la memorizzazione di file. I servizi intermediari possono essere prestati isolatamente, nel quadro di un

maggiore lo subiranno i colossi statunitensi del digitale titolari delle principali piattaforme online e motori di ricerca. Il DSA, essendo finalizzato alla fisiologica gestione della concorrenza nel mercato digitale europeo, attribuisce proprio ai fornitori di tali servizi e di motori di ricerca online di dimensioni molto grandi[15] un nutrito numero di obblighi provenienti dalle principali normative e prassi europee relative al digitale. A titolo esemplificativo, i fornitori di tali piattaforme sono gravati da diversi obblighi e ulteriori garanzie, in particolare in relazione alla moderazione dei contenuti, alla pubblicità online e ai sistemi di raccomandazione. Ciascuna di queste operazioni comporta un impatto nel come i dati personali siano utilizzati per determinare l'esperienza online dei consumatori. Pertanto, è necessario che nella progettazione e gestione dei servizi digitali i grandi operatori assicurino il rispetto della normativa sulla protezione dei dati personali[16].

Su questo fronte il DSA cerca di completare le esistenti tutele previste dal GDPR a garanzia dell'interessato[17]. Ad esempio, attraverso alcune delle misure relative alla pubblicità online e quelle sulle pratiche commerciali si integrerebbero le disposizioni del GDPR relative al consenso dell'interessato e diritto di opporsi al trattamento dei dati personali[18]. In tale frangente le prassi commerciali vietate dal DSA distorcerebbero o comprometterebbero la capacità degli interessati di compiere delle scelte o decisioni autonome informate in merito ai servizi offerti dai fornitori delle piattaforme digitali. Pertanto, con il DSA si integra il divieto delle pratiche scorrette che non sono contemplate dal GDPR estendendo la tutela degli interessati. Inoltre, viene specificatamente espresso che l'applicazione del diritto di opposizione ai trattamenti

altro tipo di servizio intermediario o simultaneamente ad altri servizi intermediari. Cfr. G. PROIETTI, *Il Digital Services Act: la normativa sui servizi digitali*, in *Diritto Bancario*, 2023, in Rete: *https://www.dirittobancario.it/art/il-digital-services-act-la-normativa-sui-servizi-digitali/*.

[15] Sostanzialmente le piattaforme gestite dai GAFAM ed ulteriori. La commissione europea ha il preciso compito di individuare tali gestori molto grandi. Questo avviene quando tali fornitori hanno un numero medio mensile di destinatari attivi nell'UE pari o superiori ai 45 milioni. La prima designazione è avvenuta il 25 aprile 2023. Le piattaforme online designate sono diciassette (Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, Zalando), mentre i motori di ricerca sono solamente due, ossia Google Search e Bing. Cfr. COMMISSIONE EUROPEA, *DSA: Piattaforme online molto grandi e motori di ricerca*, 2023, in Rete: *https://digital-strategy.ec.europa.eu/it/policies/dsa-vlops*.

[16] Cfr. EDPS, *Opinion 1/2021 on the Proposal for a Digital Services Act*, 2021, 7, in Rete: *https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf*.
D'altronde, come evidenziato dall'EDPS nel medesimo parere: "*data protection and privacy are an essential component of a vibrant digital economy, including online platforms*".

[17] Proprio nel considerano n. 10 DSA si afferma, infatti, che: "*Il presente regolamento non dovrebbe pregiudicare altri atti del diritto dell'Unione che disciplinano la prestazione di servizi della società dell'informazione in generale, che disciplinano altri aspetti della prestazione di servizi intermediari nel mercato interno o che specificano e integrano le norme armonizzate di cui al presente regolamento, […] Analogamente, per motivi di chiarezza, è opportuno che il presente regolamento non pregiudichi il diritto dell'Unione sulla tutela dei consumatori […] e sulla protezione dei dati personali, in particolare il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio*".

[18] Cfr. Art. 25 DSA: "*1. I fornitori di piattaforme online non progettano, organizzano o gestiscono le loro interfacce online in modo tale da ingannare o manipolare i destinatari dei loro servizi o da materialmente falsare o compromettere altrimenti la capacità dei destinatari dei loro servizi di prendere decisioni libere e informate. 2. Il divieto al paragrafo 1 non si applica alle pratiche contemplate dalla direttiva 2005/29/CE o dal regolamento (UE) 2016/679*".

automatizzati, compreso i processi di profilazione, ai sensi dell'art. 22 GDPR è lasciato impregiudicato ai sensi del DSA[19]. Inoltre, sempre per le misure relative alla pubblicità sulle piattaforme online e sulla profilazione, si prevedono obblighi informativi ulteriori rispetto all'art. 14 del GDPR che andranno ad illustrare le modalità di presentazione delle pubblicità, i criteri di profilazione utilizzati per profilare l'utente e i mezzi a disposizione di quest'ultimo per modificare tali criteri[20].

Il considerando n. 69[21] e l'art. 26[22] DSA, invece, prendono in considerazione i rischi determinati dai trattamenti di categorie particolari di dati ai sensi dell'art. 9 GDPR per la profilazione e il *targeting* pubblicitario, evidenziando le possibilità di discriminazione o disinformazione. Di conseguenza, i fornitori di piattaforme online dovranno stare particolarmente attenti a non svolgere trattamenti di categorie particolari di dati personali o, comunque, a dotarsi della base giuridica più idonea per procedere alla profilazione, adottando le misure più idonee ad evitare possibili violazioni dei dati che possano pregiudicare i diritti e le libertà degli interessati.

Altro elemento di interesse del DSA nel confronto con il GDPR è il trattamento dei dati dei minori. Il considerando n. 71, infatti, prevede che "*i fornitori di piattaforme online utilizzate dai minori dovrebbero adottare misure adeguate e proporzionate per proteggere i minori, ad esempio progettando le loro interfacce online o parti di esse con il massimo livello di privacy, sicurezza e protezione dei minori per impostazione predefinita, a seconda dei casi, o adottando norme per la protezione dei minori, o*

[19] Cfr. art. 25 DSA e considerando n. 68: "*[…] i fornitori di piattaforme online dovrebbero pertanto essere tenuti a provvedere affinché i destinatari del servizio dispongano di determinate informazioni personalizzate che consentano loro di comprendere quando e per conto di chi è presentata la pubblicità. […] Tali spiegazioni dovrebbero includere informazioni sul metodo utilizzato per presentare la pubblicità, ad esempio se si tratta di pubblicità contestuale o di altro tipo, e, se del caso, sui principali criteri di profilazione utilizzati; dovrebbe inoltre informare il destinatario in merito a tutti i mezzi a sua disposizione per modificare tali criteri. Le prescrizioni del presente regolamento sulla fornitura di informazioni relative alla pubblicità lasciano impregiudicata l'applicazione delle pertinenti disposizioni del regolamento (UE) 2016/679, in particolare quelle riguardanti il diritto di opposizione e il processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione, e specificamente la necessità di ottenere il consenso dell'interessato prima del trattamento dei dati personali per la L 277/18 IT Gazzetta ufficiale dell'Unione europea 27.10.2022 pubblicità mirata*".

[20] Cfr. *ibidem*.

[21] Cfr. considerando n. 69 DSA: "*In alcuni casi, le tecniche di manipolazione possono avere un impatto negativo su interi gruppi e amplificare i danni per la società, ad esempio contribuendo a campagne di disinformazione o discriminando determinati gruppi. Le piattaforme online sono ambienti particolarmente sensibili per tali pratiche e presentano un rischio per la società più elevato. Di conseguenza, i fornitori di piattaforme online non dovrebbero presentare inserzioni pubblicitarie basate sulla profilazione, come definite all'articolo 4, punto 4), del regolamento (UE) 2016/679, utilizzando le categorie speciali di dati personali di cui all'articolo 9, paragrafo 1, dello stesso regolamento, anche utilizzando categorie di profilazione basate su tali categorie speciali. Tale divieto lascia impregiudicati gli obblighi applicabili ai fornitori di piattaforme online o a qualsiasi altro fornitore di servizi o inserzionista coinvolti nella diffusione della pubblicità a norma del diritto dell'Unione in materia di protezione dei dati personali*".

[22] Cfr. art. 26 DSA: "*3. I fornitori di piattaforme online non possono presentare pubblicità ai destinatari del servizio basate sulla profilazione, quale definita all'articolo 4, punto 4), del regolamento (UE) 2016/679, utilizzando le categorie speciali di dati personali di cui all'articolo 9, paragrafo 1, del regolamento (UE) 2016/679*".

aderendo a codici di condotta per la protezione dei minori" [23], pertanto dovrebbero essere adottate misure idonee ai sensi dell'art. 8 GDPR per procedere ad un trattamento lecito dei dati del minore, in quanto capace di esprimere comunque un consenso pieno ed informato, o per escludere le inserzioni pubblicitarie basate sulla profilazione del minore, come richiesto dall'art. 28 del DSA[24].

Inoltre, permane sempre la necessità che le piattaforme digitali strutturino i loro servizi conformemente alla normativa sulla protezione dei dati personali. D'altronde, il DSA lascia impregiudicata l'applicazione completa del GDPR, come previsto dall'art. 1 DSA, perciò i diversi fornitori dovranno adottare un approccio basato sul rischio che si fondi sulla DPbDD al fine di garantire i diritti e le libertà degli interessati coinvolti nelle loro attività digitali come utenti [25]. Ad esempio, conformemente ai requisiti di minimizzazione dei dati e di protezione dei dati fin dalla progettazione, la moderazione dei contenuti non dovrebbe, per quanto possibile, comportare alcun trattamento di dati personali. Qualora sia necessario il trattamento di dati personali, ad esempio per il meccanismo di reclamo, tali dati dovrebbero riguardare solo i dati necessari per tale

[23] Cfr. considerando n. 71 DSA: "*La protezione dei minori è un importante obiettivo politico dell'Unione. I fornitori di piattaforme online utilizzate dai minori dovrebbero adottare misure adeguate e proporzionate per proteggere i minori, ad esempio progettando le loro interfacce online o parti di esse con il massimo livello di privacy, sicurezza e protezione dei minori per impostazione predefinita, a seconda dei casi, o adottando norme per la protezione dei minori, o aderendo a codici di condotta per la protezione dei minori. I fornitori di piattaforme online non dovrebbero presentare inserzioni pubblicitarie basate sulla profilazione utilizzando i dati personali del destinatario del servizio se sono consapevoli con ragionevole certezza che il destinatario del servizio è minore. Conformemente al regolamento (UE) 2016/679, in particolare al principio della minimizzazione dei dati di cui al suo articolo 5, paragrafo 1, lettera c), tale divieto non dovrebbe indurre il fornitore della piattaforma online a mantenere, acquisire o trattare un numero di dati personali superiore a quello di cui dispone già per valutare se il destinatario del servizio è un minore. Pertanto, tale obbligo non dovrebbe incentivare i fornitori di piattaforme online a rilevare l'età del destinatario del servizio prima del loro utilizzo. Dovrebbe applicarsi fatto salvo il diritto dell'Unione in materia di protezione dei dati personali*".

[24] Cfr. art. 28 DSA: "*1. I fornitori di piattaforme online accessibili ai minori adottano misure adeguate e proporzionate per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori sul loro servizio. 2. I fornitori di piattaforme online non presentano sulla loro interfaccia pubblicità basata sulla profilazione come definita all'articolo 4, punto 4), del regolamento (UE) 2016/679 che usa i dati personali del destinatario del servizio se sono consapevoli, con ragionevole certezza, che il destinatario del servizio è minore*".

[25] Cfr. considerando n. 94 DSA: "*Gli obblighi in materia di valutazione e attenuazione dei rischi dovrebbero far sorgere, caso per caso, presso i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi, la necessità di valutare e, ove necessario, adeguare la progettazione dei loro sistemi di raccomandazione, ad esempio adottando misure volte a evitare o ridurre al minimo le distorsioni che portano alla discriminazione delle persone in situazioni vulnerabili, in particolare laddove tale adeguamento sia conforme alla normativa in materia di protezione dei dati e quando le informazioni sono personalizzate sulla base di categorie particolari di dati personali di cui all'articolo 9 del regolamento (UE) 2016/679. Inoltre, e integrando gli obblighi di trasparenza applicabili alle piattaforme online per quanto riguarda i loro sistemi di raccomandazione, i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi dovrebbero provvedere in modo coerente affinché i destinatari dei loro servizi dispongano di opzioni alternative non basate sulla profilazione, ai sensi del regolamento (UE) 2016/679, per i principali parametri dei loro sistemi di raccomandazione. Tali scelte dovrebbero essere direttamente accessibili dall'interfaccia online in cui sono presentate le raccomandazioni*".

finalità specifica, applicando allo stesso tempo tutti gli altri principi del Regolamento (UE) 2016/679[26].

A fronte di tali intersezioni, è evidente che le disposizioni e misure del DSA avranno evidentemente un impatto sulla protezione dei dati personali e pertanto è necessario garantire un'efficacie complementarità tra la sorveglianza delle piattaforme online e la normativa *data protection*[27]. Sul piano pratico, questa potrebbe essere assicurata proprio dalle certificazioni rilevanti ai sensi dell'art. 42 del GDPR avente ad oggetto i trattamenti di dati personali relativi ai processi o servizi necessari per ottemperare agli obblighi del Digital Services Act. Tali meccanismi potrebbero autorevolmente asservare che i diversi trattamenti effettuati dai fornitori di servizi digitali avvengano in base dei principi della protezione dei dati e metodologicamente coerenti con i principi della *data protection by design* e *by default*, avvolgendo i sopra indicati punti di intersezione del DSA con i GDPR. Inoltre, proprio fra alcuni di questi ultimi non sarebbe necessario procedere allo sviluppo di un nuovo schema e di nuovi criteri di certificazione, ma si potrebbero adottare meccanismi di certificazione già esistenti aventi uno scopo limitato a specifici trattamenti previsti anche nel DSA. Ad esempio, rispetto al trattamento di dati dei minori o dei trattamenti di dati personali necessari per accertare l'età potrebbero già essere applicabili i meccanismi di certificazione sviluppati nel Regno Unito Age Check Certification Scheme (ACCS) e Age Appropriate Design Certification Scheme (AADCS) ove la loro applicazione venisse estesa nell'Unione europea[28].

2.2 Digital Market Act

Accanto al *Digital Services Act*, la strategia per la regolazione dei servizi digitali nel mercato dell'Unione europea ha portato all'emanazione di un ulteriore provvedimento, ossia il Regolamento (UE) 2022/1925 relativo a mercati equi e contendibili nel settore

[26] Inoltre, negli obblighi di moderazione e *Notice & Take Down* (NTD) degli *hosting provider* vi è da considerare il fatto che i fornitori delle piattaforme online potrebbero utilizzare dei sistemi di intelligenza artificiale o, comunque, dei procedimenti automatizzati per evadere il più celermente possibile i reclami formulati dagli utenti. Ciò implicherebbe l'applicazione dell'art. 22 del GDPR, il quale pone delle ferree condizioni sulle decisioni, basate su trattamenti automatizzati di dati, che possono comportare effetti giuridici o altri effetti significativi per il soggetto titolare del contenuto rimosso. Al fine di rispettare la norma in questione e promuovere la trasparenza delle proprie decisioni, l'*hosting provider* dovrebbe fornire un'informativa specifica ogniqualvolta sia utilizzato un mezzo automatizzato per l'individuazione e identificazione di contenuti illegali, indipendentemente dal fatto che la decisione finale di rimozione del contenuto illecito sia presa mediante un trattamento automatizzato o meno. Cfr. Art. 15, par. 1, lett. b)-c); EDPS, *Opinion 1/2021 on the Proposal for a Digital Services Act*, *op. cit.*, 11-12.

[27] Ciò ancor più evidente dal fatto che molte delle misure e delle ulteriori garanzie prevista dal DSA possano indirettamente contribuire ad un trattamento di dati personali, il quale rischierebbe di pregiudicare i diritti e le libertà degli interessati. Infatti, come evidenziato dall'EDPS: "*Absent further safeguards, there is a risk that the Proposal will indirectly contribute to processing of personal data, which is not proportionate to the aims pursued, in particular by not qualifying the types of illegal content that may actually warrant use of automated detection techniques involving the processing of personal data, or by not delineating the circumstances in which voluntary notification may take place*". Cfr. *ivi,* 9.

[28] Cfr. *infra*, 152. Ad esempio, attraverso l'integrazione di tali criteri di certificazione al UE-GDPR e la loro approvazione da parte dell'Autorità irlandese per la protezione dei dati (*Data Protection Commission*).

digitale (Regolamento sui mercati digitali o *Digital Market Act*, d'ora innanzi DMA)[29]. La normativa sui mercati digitali, muovendo dalla constatazione dell'applicazione difficoltosa delle norme antitrust ai suesposti mercati, interviene stabilendo una serie di obblighi in capo alle imprese di grandi dimensioni che esercitano una funzione di controllo all'accesso ai suddetti mercati. I '*gatekeeper*' – i quali vengono individuati sulla base di una serie di criteri oggettivi e molto precisi – pongono dei problemi anticoncorrenziali sistematici, in quanto, in ragione della loro posizione dominante, impediscono alle imprese europee di minori dimensioni di partecipare al mercato dei dati[30].

I *gatekeeper* sono quei portali della rete che fungono da nodo di passaggio tra le imprese digitali e i loro clienti, beneficiando, quindi, di una posizione di mercato significativa e duratura. Il regime DMA è inteso a integrare le norme vigenti in materia di concorrenza, ad affrontare più rapidamente e preventivamente i comportamenti di questi soggetti, anziché *ex post*, e a combattere le pratiche commerciali scorrette potenzialmente lesive della concorrenza. La legge sui mercati digitali impone diversi divieti e obblighi ai *gatekeeper* rivolti a: regolare l'accesso e la raccolta dei dati personali; regolamentare lo svolgimento di indagini di mercato; promuovere mercati equi e aperti e il trattamento equo dei dati personali; assicurare la condivisione dei dati generati dagli utenti commerciali e dai loro clienti nel loro utilizzo della piattaforma del *gatekeeper*[31].

Come risultato, le disposizioni del DMA produrrebbero l'effetto di rafforzare la contendibilità del mercato e, ulteriormente, anche un maggiore controllo da parte dell'interessato dei suoi dati personali[32]. Ciò può essere ricavato dagli obblighi dei *gatekeeper* previsti dagli artt. 5 e 6 del DMA. In particolare:

- l'art. 5, par. 7-8 DMA, vieta la possibilità di imporre agli utenti finali l'abbonamento obbligatorio ad altri servizi di piattaforme di base offerti dal *gatekeeper* o comunque l'utilizzo di altri servizi;
- l'art. 6, par. 3 DMA, impone al *gatekeeper* di consentire all'utente finale di disinstallare applicazioni software preinstallate sul servizio principale della piattaforma;
- l'art. 6, par. 6 DMA, che vieta al *gatekeeper* di limitare la capacità degli utenti finali di passare da un'applicazione software e da un servizio all'altro.

Ciononostante, il *gatekeeper* mantiene la piena possibilità di compiere dei trattamenti di dati personali, agendo nel rispetto delle regole dettate per la tutela della concorrenza digitale. Su questo fronte, e al pari del DSA, il DMA è rivolto ad integrare le

[29] Regolamento (UE) 2022/1925 del Parlamento Europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali), in Rete: *https://eur-lex.europa.eu/legal-content/it/txt/pdf/?uri=celex:32022r1925&qid=1691450780883*.

[30] Cfr. G.M. RUOTOLO, *Le proposte di disciplina di digital services e digital markets della Commissione del 15 dicembre 2020*, in *DPCE Online*, v. 45, n. 4, 2021, 5421, in Rete: *https://www.dpceonline.it/index.php/dpceonline/article/view/1225/1178*.

[31] Cfr. A. GAWER, *Digital platforms and ecosystems: remarks on the dominant organizational forms of the digital age*, in *Innovation: Organization & Management*, 2022, Vol. 24, N. 1, 110-124, in Rete: *https://doi.org/10.1080/14479338.2021.1965888*.

[32] Cfr. EDPS, *Opinion 2/2021 on the Proposal for a Digital Markets Act*, 2021, in Rete: *https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_markets_act_en.pdf*.

norme del GDPR, prevedendo delle regole specifiche per i trattamenti di dati personali compiuti nel contesto dei servizi di piattaforma offerti dai *gatekeeper*[33]. Pertanto, a fronte dell'elevata complessità e specificità della materia, è da ritenersi ragionevolmente che, attualmente, le certificazioni previste dal GDPR non possano ritenersi sufficienti ad attestare la conformità di tali operatori alle norme sulla protezione dei dati personali come integrate dal DMA. Piuttosto i principi previsti dagli artt. 42 e 43 del Reg. (UE) 2016/679 potranno essere usate come base per l'adozione di un meccanismo specifico di attuazione del DMA basato sull'autoregolamentazione o sulla co-regolamentazione, come codici di condotta o certificazioni. Tuttavia, questo è subordinato all'individuazione di criteri di certificazione ulteriori e aderenti ai requisiti della legge sui mercati digitali, che permettano di attestare la conformità dei *gatekeeper*.

3 La Strategia europea per i dati: come coniugare la libera circolazione dei dati con le Certificazioni GDPR

3.1 Data Governance Act

Il 30 maggio 2022 è stato ufficialmente promulgato il *Data Governance Act*, ossia il Regolamento (UE) 2022/868 relativo alla governance europea dei dati (d'ora in avanti DGA)[34]. Il DGA fa parte del più ampio quadro normativo predisposto dall'UE per la digitalizzazione, lo sviluppo dell'economia digitale dei dati, per l'intelligenza artificiale e altri importanti obiettivi rivolti allo sviluppo di una sovranità digitale europea. Come detto in introduzione, dopo l'emanazione del GDPR, negli ultimi anni l'attenzione si è spostata verso la facilitazione dell'economia dei dati e della loro condivisione in Europa.

[33] Ad esempio, proprio l'art. 5, par. 2 DMA si prevede, quali obblighi generali, che: "*Il gatekeeper: a) non tratta, ai fini della fornitura di servizi pubblicitari online, i dati personali degli utenti finali che utilizzano servizi di terzi che si avvalgono di servizi di piattaforma di base del gatekeeper; b) non combina dati personali provenienti dal pertinente servizio di piattaforma di base con dati personali provenienti da altri servizi di piattaforma di base o da eventuali ulteriori servizi forniti dal gatekeeper o con dati personali provenienti da servizi di terzi; c) non utilizza in modo incrociato dati personali provenienti dal pertinente servizio di piattaforma di base in altri servizi forniti separatamente dal gatekeeper, compresi altri servizi di piattaforma di base, e viceversa; e d) non fa accedere con registrazione gli utenti finali ad altri servizi del gatekeeper al fine di combinare dati personali, a meno che sia stata presentata all'utente finale la scelta specifica e quest'ultimo abbia dato il proprio consenso ai sensi dell'articolo 4, punto 11), e dell'articolo 7 del regolamento (UE) 2016/679. Se l'utente finale ha negato o revocato il consenso prestato ai fini del primo comma, il gatekeeper non ripete la sua richiesta di consenso per la stessa finalità più di una volta nell'arco di un anno. Il presente paragrafo lascia impregiudicata la possibilità per il gatekeeper di avvalersi dell'articolo 6, paragrafo 1, lettere c), d) ed e), del regolamento (UE) 2016/679, se del caso*".

[34] Regolamento (UE) 2022/868 del Parlamento Europeo e del Consiglio del 30 Maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati), 2022, in Rete: *https://eur-lex.europa.eu/legal-content/it/txt/html/?uri=celex:32022r0868*. Il regolamento avrà piena applicabilità a partire dal settembre 2023. Per approfondire gli aspetti principali del DGA v. E. SALERNO, *Il Data Governance Act, il nuovo Regolamento europeo per il mercato unico dei dati rischia di non essere abbastanza e favorire i grandi della tecnologia*, 2021, in Rete: https*://www.researchgate.net/publication/350286221*.

A tal fine, il regolamento in questione cerca di facilitare l'ulteriore condivisione dei dati personali introducendo il concetto di altruismo dei dati.

Con il DGA, la Commissione ha inteso creare uno spazio europeo dei dati affidabile e per facilitare la circolazione e l'uso dei dati per la ricerca e la creazione di nuovi servizi e prodotti innovativi nel settore sia pubblico che privato. Il DGA si poggia fondamentalmente su tre pilastri: il primo è relativo all'introduzione della disciplina per il riutilizzo dei dati protetti detenuti da soggetti pubblici. Il secondo pilastro è, invece, rappresentato dall'introduzione di un nuovo quadro regolativo per il controllo di servizi di intermediazione dei dati, ossia di servizi che avranno come obiettivo la condivisione negli spazi europei dei dati sia personali che non personali[35]. Il terzo pilastro concerne invece l'introduzione del c.d. 'altruismo dei dati', ovverosia di un meccanismo per facilitare i privati e i soggetti pubblici a rendere volontariamente disponibili i dati personali e non personali per finalità altruistiche[36].

Il fatto di incentivare la condivisione e la circolazione dei dati, tuttavia, non esclude il fatto che ai dati personali rimane comunque applicabile il GDPR. Proprio il Regolamento sulla protezione dei dati personali ha un ruolo fondamentale nel DGA, venendo richiamato più volte direttamente e indirettamente, attraverso la disciplina di condivisione e riutilizzo dei dati.

In particolare, l'art. 5 DGA, il quale detta le condizioni per il riutilizzo dei dati, prevede che per garantirne l'adeguata protezione, gli enti pubblici devono assicurare che questi siano resi anonimi. I dati personali, quindi, devono essere sottoposti ad un processo adeguato di anonimizzazione per poi consentire il loro riutilizzo uscendo, di fatto, dalla portata applicativa del GDPR[37]. Tuttavia, a fronte dell'evoluzione delle tecniche computazionali e dell'intelligenza artificiale, bisognerebbe interrogarsi su come e quanto un dato personale possa considerarsi anonimizzato. A fronte dell'evoluzione delle citate tecniche, infatti, sarebbe maggiormente semplice rintracciare ulteriori informazioni relative all'interessato che sommate ai dati anonimi permetterebbero di reidentificarlo[38]. Contro questa criticità le certificazioni ai sensi del GDPR, o in generale altri schemi di standardizzazione, potrebbero essere dei meccanismi affidabili per constatare l'efficace anonimizzazione dei dati personali. D'altronde, dato che anche il

[35] Cfr. Art. 2, n. 11 DGA: "*«servizio di intermediazione dei dati»: un servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali […]*".

[36] L'altruismo dei dati si basa sull'autorizzazione fornita da un'organizzazione per attività di trattamento senza scopo di lucro di dati non personali o sulla nozione di consenso nel caso in cui siano coinvolti dati personali. Per la definizione completa, v. art. 2, n. 16 DGA.

[37] Proprio il medesimo articolo, inoltre, vieta agli utenti che riutilizzino i dati anonimizzati di procedere ad un qualunque tentativo di re-identificazione degli interessati, proprio perché si svilupperebbe un trattamento illecito di dati personali ai sensi del GDPR.

[38] Proprio sul punto, e sulla differenza tra anonimizzazione e pseudoanonimizzazione è recentemente intervenuto il Tribunale dell'Unione europea con la sentenza pronunciata nella causa T-557/20 con il quale ha stabilito che i dati pseudonimizzati trasmessi a un destinatario non possono essere considerati dati personali, rimanendo quindi anonimi, se il destinatario non dispone di mezzi legali concretamente realizzabili che gli consentano di accedere alle informazioni aggiuntive, necessarie per poter reidentificare gli interessati (Trib. I Grado Unione europea, Sez. VIII ampliata, Sent., 26/04/2023, n. 557/20, in *OneLegale*).

procedimento di anonimizzazione è un trattamento di dati personali che, pertanto, deve fondarsi su una delle condizioni di liceità dell'art. 6 GDPR e rispettare gli altri obblighi previsti dal Reg. (UE) 2016/679, ben può costituire oggetto di una certificazione *ex* art. 42 GDPR[39]. Pertanto, la certificazione di un'efficace modalità di anonimizzazione dei dati personali può essere fondamentale per prevenire la de-anonimizzazione e i tentativi di reidentificazione dell'interessato, permettendo l'efficace attuazione del DGA. Quest'ultimo, infatti, sponsorizzando il riutilizzo e la condivisione dei dati, ove questi ultimi fossero informazioni personali, entrerebbe in conflitto con uno dei principi fondanti del GDPR, ossia il principio di limitazione delle finalità[40]. Pertanto, fuori dai casi di trattamento ulteriore dei dati personali per una finalità ulteriore di ricerca storica, scientifica o statistica, il riutilizzo dei dati personali sarebbe impossibile in assenza di una corretta anonimizzazione[41].

Altro rilevante tema è quello dei servizi di intermediazione dei dati. Come detto, questi mirano a stabilire relazioni commerciali ai fini della condivisione dei dati. L'obiettivo è quello di promuovere lo scambio di dati tramite piattaforme, banche dati e infrastrutture di dati in generale attraverso protocolli e formati di dati comuni che garantiscano l'interoperabilità e la sicurezza [42]. Il fatto che questi servizi di intermediazione dei dati possano avere ad oggetto anche dati personali non anonimizzati determina un trattamento e quindi l'applicazione del GDPR e di tutte le garanzie ivi previste[43]. Al fine di rendere il trattamento svolto dalle organizzazioni che offrono servizi di intermediazione dei dati conformi al Reg. (UE) 2016/679 questi potranno aderire ad un meccanismo di certificazione *ex* art. 42 GDPR.

3.2 Data Act

[39] Cfr. M. MASSIMINI, *Anonimizzazione dei dati personali: significato, benefici e dubbi in ottica GDPR*, 2021, in *Privacy.it*, in Rete: *https://www.privacy.it/2021/05/11/anonimizzazione-gpdr-massimini/#:~:text=L%27anonimizzazione%20%C3%A8%2C%20come%20detto,tra%20quelle%20elencate%20all%27art*.

[40] Cfr. Art. 5, par. 1, lett. b) GDPR: "*I dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»)*".

[41] Cfr. J. RUOHONEN, S. MICKELSSON, *Reflections on the Data Governance Act*, in *Digital Society (DISO)*, 2, 10, 2023, 5-6, in Rete: *https://doi.org/10.1007/s44206-023-00041-7*.

[42] In particolare, ai sensi dell'art. 12, lett. e) DGA: "*i servizi di intermediazione dei dati possono comprendere l'offerta di strumenti e servizi supplementari specifici ai titolari dei dati o agli interessati allo scopo specifico di facilitare lo scambio dei dati, come la conservazione temporanea, la cura, la conversione, l'anonimizzazione e la pseudonimizzazione, fermo restando che tali strumenti e servizi sono utilizzati solo su richiesta o approvazione esplicita del titolare dei dati o dell'interessato e gli strumenti di terzi offerti in tale contesto non utilizzano i dati per altri scopi*".

[43] Cfr. Art. 1, par. 3 DGA: "*Il diritto dell'Unione e nazionale in materia di protezione dei dati personali si applica a qualsiasi dato personale trattato in relazione al presente regolamento. In particolare, il presente regolamento non pregiudica i regolamenti (UE) 2016/679 e (UE) 2018/1725 e le direttive 2002/58/CE e (UE) 2016/680 […]. Il presente regolamento non crea una base giuridica per il trattamento dei dati personali e non influisce sui diritti e sugli obblighi di cui ai regolamenti (UE) 2016/679 e (UE) 2018/1725 o alle direttive 2002/58/CE o (UE) 2016/680*".

Il 23 febbraio 2022 la Commissione europea ha proposto la c.d. "legge sui dati" (*Data Act*, di seguito DA) nell'ambito della strategia europea in materia di dati[44]. La DA è una risposta alla scarsa fiducia nella condivisione dei dati, agli incentivi economici contrastanti e agli ostacoli tecnologici per consolidare e sviluppare una *data economy* europea basata su dati industriali non personali derivanti dalla proliferazione di prodotti connessi all'*Internet of things*[45]*.* La proposta di regolamento in tema mira a stabilire norme uniformi per consentire l'accesso, il riutilizzo e la condivisione dei dati originati dall'uso di un prodotto o di un servizio IT da parte di un utente, nonché alla messa a disposizione di dati da parte dei titolari degli stessi prodotti dai medesimi dispositivi[46]. Dunque, l'ambito di applicazione previsto della proposta non riguarda esclusivamente i dati personali, ma si applicherebbe piuttosto ai dati personali e non personali generati dall'uso di prodotti e servizi ai sensi della proposta. Tuttavia, anche ove fossero parzialmente coinvolti dati personali, il regolamento proposto intente comunque assicurare un elevato livello di protezione dei dati personali.

La presente proposta, tuttavia, pone delle norme che si collegano al GDPR, rischiando potenzialmente di sovrapporsi ad esso:

- il DA, infatti, crea all'art. 3 un obbligo di condivisione dei dati in situazioni precedentemente non contemplate dal GDPR o da altri atti dell'Unione. Questo obbligo mira a promuovere, per impostazione predefinita, la condivisione dei dati non personali generati dai dispositivi *smart* connessi all'IoT verso soggetti terzi in modo facile e sicuro. Questo obbligo dovrebbe uniformare la progettazione dei prodotti e servizi digitali, al fine di rendere interoperabili i dati generati dagli utenti attraverso i dispositivi connessi alla rete[47];
- all'art. 4, invece, la proposta pone un nuovo diritto di accesso agli utenti[48] dei prodotti *smart*, che siano anche interessati al trattamento, ai propri dati generati tramite il medesimo dispositivo. Questo nuovo diritto è completato da ulteriori garanzie nel caso in cui l'utente richiedente i dati personali non sia un interessato, ma ad esempio un'impresa[49]. Quest'ultima, infatti, sarà considerata come titolare del trattamento ai sensi del GDPR, perciò, qualora intenda richiedere l'accesso ai

[44] COMMISSIONE EUROPEA, *COM/2022/68, Proposta di Regolamento del Parlamento Europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati)*, 2022, in Rete: *https://eur-lex.europa.eu/legal-content/it/txt/pdf/?uri=celex:52022pc0068*.

[45] Cfr. *ivi* (Relazione alla proposta di regolamento), 1.

[46] Per maggiori approfondimenti si v. A. FERNANDEZ, *The Data Act: The next Step in Moving Forward to a European Data Space*, in *European Data Protection Law Review (EDPL)*, 8, n. 1, 2022, 108-114, in Rete: *https://edpl.lexxion.eu/article/EDPL/2022/1/16*.

[47] Cfr. art. 3, par. 1 DA: "*I prodotti sono progettati e fabbricati e i servizi correlati sono forniti in modo tale che i dati generati dal loro uso siano, per impostazione predefinita, accessibili all'utente in modo facile, sicuro e, ove pertinente e opportuno, diretto".* Inoltre, vengono previsti una serie di oneri informativi che devono essere forniti all'utente del prodotto o servizio IoT rispetto ai possibili dati che possono essere generali, le modalità di accesso e la possibilità di condivisione dei medesimi dati.

[48] I quali possono essere sia persone fisiche (e quindi interessati da un possibile trattamento) o persone giuridiche (quali altre imprese). Cfr. art. 2, n. 5 DA.

[49] Cfr. Art. 4, par. 5 DA: "*Se l'utente non è un interessato, i dati personali generati dall'uso di un prodotto o di un servizio correlato sono messi a disposizione dell'utente dal titolare dei dati solo se esiste una base giuridica valida a norma dell'articolo 6, paragrafo 1, del regolamento (UE) 2016/679 e, ove pertinente, se sono soddisfatte le condizioni di cui all'articolo 9 del regolamento (UE) 2016/679*".

dati personali, sarà tenuta a disporre di una base giuridica idonea per il trattamento dei dati ai sensi dell'art. 6, par. 1, o dell'art. 9 GDPR. In questo modo, questo diritto di accesso ai dati prodotti dai dispositivi *smart* non pregiudicherebbero i diritti e le libertà protette dal GDPR[50]. Infine, altra possibilità è che il *dataset* composto dai dati dell'utente-persona fisica ricomprenda sia dati non personali, sia dati personali. In tale circostanza il *Data Act* garantisce l'applicazione delle norme sul GDPR[51];

- altro punto di contatto è con il diritto alla portabilità dei dati previsto dall'art. 20 del GDPR. Il DA evidenzia espressamente all'art. 1 par. 3 che "*qualora gli utenti siano gli interessati di dati personali soggetti ai diritti e agli obblighi di cui a tale capo, le disposizioni del presente regolamento integrano il diritto alla portabilità dei dati di cui all'articolo 20 del regolamento (UE) 2016/679*". In particolare, le norme del DA integrerebbero in vari modi il diritto alla portabilità dei dati, conferendo agli utenti-interessati "*il diritto di accedere a tutti i dati generati dall'uso di un prodotto o di un servizio correlato, e di metterli a disposizione di terzi, indipendentemente dalla loro natura di dati personali, dalla distinzione tra dati forniti attivamente o osservati passivamente e dalla base giuridica del trattamento*"[52].

[50] Cfr. considerando n. 30 DA: "*[…] Se l'utente non è l'interessato ma un'impresa, compreso un operatore commerciale individuale, e non nei casi di uso domestico condiviso del prodotto, l'utente sarà un titolare del trattamento ai sensi del regolamento (UE) 2016/679. Di conseguenza tale utente, in qualità di titolare del trattamento che intenda richiedere dati personali generati dall'uso di un prodotto o di un servizio correlato, deve disporre di una base giuridica per il trattamento dei dati a norma dell'articolo 6, paragrafo 1, del regolamento (UE) 2016/679, come il consenso dell'interessato o un legittimo interesse. Tale utente dovrebbe garantire che l'interessato sia adeguatamente informato delle finalità specificate, esplicite e legittime del trattamento di tali dati e del modo in cui l'interessato può effettivamente esercitare i propri diritti. Il titolare dei dati e l'utente, se sono contitolari del trattamento ai sensi dell'articolo 26 del regolamento (UE) 2016/679, sono tenuti a determinare in modo trasparente, mediante un accordo tra loro, le rispettive responsabilità in materia di conformità a tale regolamento. Dovrebbe restare inteso che tale utente, una volta resi disponibili i dati, può a sua volta diventare titolare dei dati se soddisfa i criteri di cui al presente regolamento e divenire così soggetto all'obbligo di mettere a disposizione i dati a norma del presente regolamento"*.

[51] Proprio sulla natura dei dati coinvolti nel *Data Act* si fonda la principale critica della proposta. Infatti, il *Data Act* prende principalmente in considerazione una nozione imprecisa di dati generati dai prodotti o servizi dell'IoT, definiti, dall'art. 1, par. 2 della proposta come "*qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi compilazione di tali atti, fatti o informazioni, anche in forma sonora, visiva o registrazione audiovisiva*". È evidente che, visto lo scopo del regolamento, si sia voluto prendere a riferimento dati non personali in quanto non riconducibili ad un individuo. Tuttavia, il GDPR prende a riferimento una nozione più ampia di dato personale, ricomprendendo non solo le informazioni direttamente riferibili ad una persona fisica, ma anche quelle apparentemente non riconducibili (da sole) ad un individuo che però permettono di identificarlo indirettamente. Prendendo a riferimento questa definizione, il campo applicativo del DA andrebbe a sovrapporsi a quello del GDPR, rendendo difficoltosa l'applicazione di entrambi i regolamenti. Cfr. EDPB-EDPS, *Parere congiunto EDPB-GEPD 2/2022 sulla proposta del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati)*, 2022, 13-14, in Rete: *https://edpb.europa.eu/system/files/2023-03/edpb-edps_jointopinion_2022-02_data_act_proposal_it.pdf*.

[52] Cfr. considerando n. 31 DA. Inoltre, sempre rispetto a quanto indicato dal considerando menzionato, il *Data Act*, impone e garantisce la fattibilità tecnica dell'accesso di terzi a tutti i tipi di dati che rientrano nel suo ambito di applicazione, siano essi personali o non personali. Consente inoltre al titolare dei dati di fissare un compenso ragionevole a carico di terzi, ma non dell'utente, per eventuali costi sostenuti per

Ecco, quindi, che rispetto alle intersezioni sopra individuate le certificazioni ai sensi del GDPR potrebbero essere un valido punto di appoggio per permettere ai titolari e ai responsabili del trattamento di adeguare la propria organizzazione a rispondere agli obblighi previsti dal *Data Act* in tema di condivisione di dati personali. Inoltre, proprio per il fatto che le due normative rischierebbero di sovrapporsi, anche a fronte della criticata nozione di dato ai sensi del DA, aderire ad un meccanismo di certificazione permetterebbe di definire meglio la tipologia di dati gestiti e/o trattati dai prodotti o servizi legati all'IoT. Questo, ad esempi, potrebbe avvenire valutando se un determinato trattamento di dati rientri nel ToE preso in considerazione da un meccanismo di certificazione e dai relativi criteri. Tuttavia, attualmente, data l'assenza di schemi di certificazione rivolti al trattamento di dati personali compiuto in prodotti, processi o servizi legati all'IoT risulta difficile fare ulteriori previsioni in merito alla commistione tra gli obblighi del *Data Act* e le certificazioni ai sensi del GDPR.

4 La proposta di Regolamento sull'intelligenza artificiale e la possibile applicazione delle certificazioni ai sensi del GDPR

La protezione dei dati personali nello sviluppo di un'intelligenza artificiale è un tema fondamentale. Le applicazioni basate sull'IA forniscono nuove e preziose soluzioni per affrontare i bisogni e le sfide in molti ambiti, quali la domotica, le *smart cities*, l'industria, la sanità e la prevenzione del crimine. Tuttavia, per raggiungere tali soluzioni è necessario che i sistemi di IA vengano addestrati sulla base di una grande mole di dati, i quali costituiscono la base di partenza per arrivare ad ogni risultato computazionale. L'importanza dei dati per lo sviluppo di IA, e in particolare per quelle basate su un approccio *machine learning*[53], determina che, contrariamente a una visione diffusa, l'opportunità di un intervento legislativo dovrebbe essere richiesta non tanto nella regolamentazione degli algoritmi quanto nella disciplina dei dati di addestramento dell'IA.

Tale argomento è stato affrontato anche da fonti di carattere internazionale, quale la Convenzione 108 del Consiglio d'Europa, attraverso cui si è cercato di introdurre delle linee guida che potessero sostenere lo sviluppo etico dell'IA tenendo, soprattutto, in considerazione i principi e le garanzie fondamentali della *data protection*[54]*.* Tuttavia, a fronte delle recenti innovazioni digitali e computazionali, nonché dal rischio che il mercato europeo possa essere indelebilmente influenzato da altri ecosistemi giuridico-

fornire un accesso diretto ai dati generati dal prodotto dell'utente. Se un titolare dei dati e un terzo non sono in grado di concordare le condizioni di tale accesso diretto, all'interessato non dovrebbe essere in alcun modo impedito di esercitare i diritti di cui al regolamento (UE) 2016/679, compreso il diritto alla portabilità dei dati, esperendo i mezzi di ricorso in conformità a tale regolamento. In tale contesto resta inteso che, conformemente al regolamento (UE) 2016/679, un accordo contrattuale non consente il trattamento di categorie particolari di dati personali da parte del titolare dei dati o del terzo.

[53] In merito alla differenza tra le modalità di addestramento delle IA, v. IBM, *AI vs. Machine Learning vs. Deep Learning vs. Neural Networks: What's the difference?*, in Rete: *https://www.ibm.com/blog/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks/*.

[54] Cfr. CONSIGLIO D'EUROPA, *(Convenzione 108) Linee-Guida in materia di intelligenza artificiale e protezione dei dati*, 2019, in Rete: *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9096716*.

economici (come quello americano o cinese), hanno comportato l'intervento della Commissione attraverso la proposizione di un regolamento omnicomprensivo sull'IA. Il 21 aprile 2021 la Commissione europea ha presentato la propria proposta di regolamento rivolta a stabilire delle regole armonizzate sull'intelligenza artificiale (*Artificial Intelligence Act*, d'ora in poi AIA)[55], ossia il primo tentativo legislativo al mondo di normare la tecnologia dell'intelligenza artificiale in tutti i suoi aspetti[56].

A fronte di tale premessa è necessario sottolineare come il presente contributo non ha lo scopo di compiere una trattazione esaustiva della nuova proposta di regolamento. L'obiettivo di questo capitolo, infatti, è di analizzare i collegamenti normativi che sorgono tra il testo della proposta e il GDPR, rispetto al possibile utilizzo dei dati personali per l'addestramento delle IA, nonché a evidenziare i possibili spazi applicativi delle certificazioni ai sensi del GDPR nella regolamentazione dell'intelligenza artificiale. A tal fine, è comunque necessario procedere ad una breve analisi della nuova proposta di regolamento.

Come anticipato, l'AIA intende dettare delle regole per lo sviluppo, l'immissione sul mercato o la messa in servizio di sistemi di IA nell'UE. La nozione di intelligenza artificiale adottata dalla proposta di regolamento è al quanto generica, intendendosi come tale "*un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono*"[57].

Posto ciò, l'approccio adottato dalla Commissione nell'AIA è totalmente basato sul rischio, ossia prendendo in considerazione i possibili pregiudizi che gli individui

[55] Cfr. COMMISSIONE EUROPEA, *COM/2021/206, Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione*, 2021, in Rete: *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206*.

[56] La proposta di regolamento sull'IA è stata approvata, in prima lettura, dal Parlamento europeo il 14 giugno 2023. Subito dopo il voto, con un primo accordo politico tra il Parlamento, la Commissione e il Consiglio, è stato indetto il primo trilogo sulla proposta di regolamento sull'IA prima della presa di posizione del Consiglio dell'UE (c.d. *early-second reading agreements*). Ai negoziatori del primo trilogo è stato conferito un ampio mandato per discutere su tutti gli aspetti tecnici della proposta. A fronte dell'esame della proposta da parte dei rappresentanti del Parlamento, Consiglio e Commissione è stato pubblicato il 2 agosto 2023 un primo documento contenente le revisioni e le modifiche proposte per il progetto di regolamento sull'IA. Per approfondire l'ultima versione della proposta di regolamento sull'IA v. COUNCIL OF THE EUROPEAN UNION, *Interinstitutional File: 2021/0106(COD)*, 10.07.2023 (pubblicato il 02.08.2023), in Rete: *https://data.consilium.europa.eu/doc/document/ST-11320-2023-REV-1/en/pdf*.

[57] Cfr. art. 3, n. 1 AIA. L'allegato I della proposta di regolamento prevede poi le 'tipologie' di intelligenze artificiali rientranti nell'ambito applicativo dell'AIA, ossia: "*a) Approcci di apprendimento automatico, compresi l'apprendimento supervisionato, l'apprendimento non supervisionato e l'apprendimento per rinforzo, con utilizzo di un'ampia gamma di metodi, tra cui l'apprendimento profondo (deep learning); b) approcci basati sulla logica e approcci basati sulla conoscenza, compresi la rappresentazione della conoscenza, la programmazione induttiva (logica), le basi di conoscenze, i motori inferenziali e deduttivi, il ragionamento (simbolico) e i sistemi esperti; c) approcci statistici, stima bayesiana, metodi di ricerca e ottimizzazione*". Il fatto che la definizione delle 'tecniche' di intelligenza artificiale sia posta in un allegato alla proposta di regolamento, così come altri elementi importanti dell'AIA, è dovuto al fatto di semplificare in futuro le modalità di modifica del regolamento, il quale potrà avvenire con atti delegati della Commissione al posto del procedimento legislativo di modifica ordinario.

potrebbero subire in relazione ad un determinato utilizzo dell'IA[58]. Vengono, quindi, previsti quattro livelli di rischio che determinano l'applicazione di obblighi e garanzie differenti. Nel primo livello, ossia quello con il grado di rischio più elevato, l'AIA identifica le pratiche di IA vietate[59]. Nel secondo livello, invece, vengono classificati gli impieghi dell'IA ad alto rischio. La classificazione di un sistema di IA ad alto rischio viene svolta sulla base del fatto che questa costituisca un componente di un prodotto o sia essa stessa un prodotto *stand-alone* rientrante negli atti dell'Unione previsti nell'allegato II della proposta, oppure che, sulla base delle sue funzioni, rientri in uno dei settori presenti nell'allegato III. Per gli utilizzi ad alto rischio dell'IA, la proposta di regolamento prevede un articolato sistema di *governance* relativo a tutti i requisiti che devono essere rispettati per consentire lo sviluppo, l'immissione sul mercato e l'utilizzo dell'applicativo. Infine, nel terzo e quarto livello vengono fatti rientrare i sistemi a basso o a rischio minimo[60], per i quali vengono previsti degli obblighi di trasparenza e informativa agli utenti con cui interagiscono[61].

[58] L'approccio adottato dall'AIA è apparentemente simile con quello del GDPR. Pur essendo, infatti, fondate sul *risk based approach* i regolamenti differiscono in base al fatto che nella proposta sull'IA è il legislatore comunitario che individua preventivamente il rischio relativo alle pratiche di IA, prevedendo, a seconda dei casi, obblighi diversi. Mentre nel GDPR è il titolare del trattamento che dovrà autonomamente analizzare la rischiosità del trattamento di dati personali operato, prevedendo, a seconda del caso concreto, misure tecniche ed organizzative differenti volte a mitigare gli eventuali pregiudizi causabili all'interessato dal trattamento.

[59] Cfr. art. 5 AIA. In particolare, la proposta vieta l'utilizzo di sistemi IA che sfruttino tecniche subliminali o le vulnerabilità di determinati gruppi di persone, al fine di distorcerne il comportamento in modo da provocare ai soggetti coinvolti o ad altri un danno fisico o psicologico; i sistemi di *social scoring* utilizzati dalle autorità pubbliche per classificare l'affidabilità delle persone, in cui il punteggio sociale ottenuto abbia come conseguenza il trattamento pregiudizievole o sfavorevole di determinate persone o gruppi di persone in contesti sociali non collegati ai contesti in cui i dati sono stati originariamente raccolti, o un trattamento pregiudizievole o sfavorevole ingiustificato o sproporzionato rispetto al comportamento sociale delle persone oggetto di valutazione o rispetto alla gravità di tale condotta. Infine, vengono vietati i sistemi di identificazione biometrica "in tempo reale" e in spazi aperti al pubblico per finalità di polizia, a meno che non siano strettamente necessari per la ricerca mirata di potenziali vittime di azioni criminose, per la prevenzione di un pericolo specifico, sostanziale e imminente alla vita o alla sicurezza di una persona o di un attacco terroristico o, infine, per la individuazione, localizzazione o incriminazione di un soggetto sospetto di reati gravi. In ogni caso il ricorso di questi sistemi dovrebbe essere autorizzato dall'autorità giudiziaria o da un'autorità amministrativa indipendente, a seguito di richiesta motivata.
A fronte della prima approvazione della proposta dal Parlamento europeo, fra le altre modifiche, i sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico sono stati integralmente vietati. Per le attività di *law enforcement* rimangono ammissibili le pratiche di sistemi di IA volte all'identificazione biometrica a distanza "a posteriori", ma solo per il perseguimento di reati gravi e previa autorizzazione dell'autorità giudiziaria. Inoltre, a fronte del fenomeno di ChatGPT, sono stati introdotti ulteriori obblighi per i sistemi di IA generativa volti a garantire maggiore trasparenza e a introdurre salvaguardie contro la generazione di contenuti illeciti. Cfr. EUROPEAN PARLIAMENT, *Legislative Observatory: Artificial Intelligence Act*, 14.06.2023, in Rete: *https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1747977&t=e&l=en*.

[60] Cfr. art. 52 AIA. Tale categoria di IA è residuale e ricavabile al negativo, venendo classificati come sistemi a basso o rischio minimo tutti quelli che non sono vietati e non sono ad alto rischio.

[61] Cfr. C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw Journal – Rivista di BioDiritto*, n. 3/2021, 9, in Rete: *https://iris.unitn.it/retrieve/handle/11572/318571/516882/document(1).pdf*.

Come preannunciato, la maggior parte della proposta di regolamento sull'IA (Titolo III) si concentra sulle regole applicabili ai sistemi di IA ad alto rischio, prevedendo una struttura di *governance* complessa volta a ridurre al massimo i pericoli per i diritti degli utenti. Fra le regole previste per la messa in servizio di un sistema di IA ad alto rischio vi sono anche alcuni requisiti relativi alla *data protection*. La legge sull'IA lascia impregiudicata l'applicazione della normativa europea in materia di materia di protezione dei dati, pertanto, ogni trattamento di dati personali compiuto dovrà sottostare agli obblighi e garanzie del GDPR[62]. Pertanto, l'utente di un sistema di IA, qualificabile come titolare del trattamento, potrà effettuare un trattamento di dati personali solo mediante una legittima base giuridica del trattamento, dovrà svolgere una valutazione d'impatto sulla protezione dei dati personali (considerando le caratteristiche tecniche e il caso d'uso in cui l'IA è coinvolta), dovrà sottoscrivere un accordo di trattamento con il fornitore del sistema, il quale potrà essere qualificato come responsabile del trattamento, dovrà adottare ogni misura tecniche ed organizzativa di sicurezza volta ad assicurare l'integrità dei dati trattati e a prevenire ogni possibile violazione e, infine, dovrà salvaguardare la garanzia prevista dall'art. 22 GDPR. Rispetto a tale contesto, quindi, le certificazioni previste dal Reg. (UE) 2016/679 potrebbero ben applicarsi. Ovviamente i criteri di certificazione dovranno prevedere controlli specifici per i trattamenti compiuti mediante sistemi di IA al fine di attestarne la conformità con i principi della protezione dei dati personali[63].

Tuttavia, rispetto ai trattamenti automatizzati di dati compiuti mediante IA, permangono alcuni fondamentali problemi, come quello della spiegabilità delle decisioni prese dall'algoritmo. Ai sensi dell'art. 5, par. 1, lett. a), gli interessati dovrebbero sempre ricevere una spiegazione generale della logica dell'algoritmo e dell'ambito di applicazione dell'IA, al fine anche di esercitare coscientemente i propri diritti. Ciononostante, non sempre è possibil dare una spiegazione certa delle decisioni prese dal sistema automatizzato, comprimendo necessariamente il principio di trasparenza[64]. Sul punto la proposta prevede che ogni sistema ad alto rischio sia disegnato e sviluppato in modo da assicurare un appropriato livello di trasparenza. Per

[62] Cfr. considerando n. 41 AIA, il quale specifica, per l'appunto, che il fatto che un'IA sia classificata ad alto rischio non rende automaticamente lecito l'utilizzo del medesimo, ma al contrario esso dovrà conformarsi alla legislazione europea e nazionale, compresa quella sulla protezione dei dati personali.

[63] Cfr. N. MARSCH, *Artificial Intelligence and the Fundamental Right to Data Protection: Opening the Door for Technological Innovation and Innovative Protection*, in T. WISCHMEYER, T. RADEMACHER (a cura di), *Regulating Artificial Intelligence*, 34-50, 2020, in Rete: *https://link.springer.com/book/10.1007/978-3-030-32361-5*; EDPB-EDPS, *Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale)*, 2021, 14-15, in Rete: *https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_it.pdf*.

[64] Il problema della *blackbox* rappresenta l'elemento più problematico, concernendo principalmente i sistemi avanzati di IA basati sul *machine learning* o *deep learning*. Tali dispositivi, infatti, sono caratterizzati da una estrema complessità che rende praticamente impossibile tracciare la catena dei passaggi seguiti per generare il risultato finale. L'opacità del procedimento decisionale di queste macchine determina l'impossibilità di verificare la congruità delle decisioni assunte dal sistema. Per approfondire v. A. BIBAL, M. LOGNOUL, A. DE STREEL, B. FRÉNAY, *Legal requirements on explainability in machine learning*, in *Artificial Intelligence and Law*, 29, 2021, 149-169, in Rete: *https://link.springer.com/article/10.1007/s10506-020-09270-4*.

adottare misure proporzionate a 'spiegare' la decisione algoritmica, o almeno la logica in base al quale è stata presa, l'adesione ad un meccanismo di certificazione potrebbe rappresentare un *feedback* importante per verificare la correttezza della metodologia utilizzata per far fronte a tale onere.

Rispetto alla *governance* dei dati personali, il GDPR non è l'unica fonte normativa da prendere in considerazione. La proposta, infatti, introduce dei requisiti nuovi e complementari a quanto già previsto che il fornitore[65] sarà tenuto a soddisfare per l'addestramento del sistema di IA ad alto rischio. Ai sensi dell'art. 10 AIA, i sistemi di IA ad alto rischio basati su tecniche di apprendimento dai dati devono soddisfare alcuni criteri di qualità, in particolare per quanto riguarda i dati per l'addestramento (*data set*), per la convalida (*validation set*) e per la prova (*test set*). I dati devono essere pertinenti, rappresentativi, esenti da errori e completi; inoltre, devono tenere conto delle proprietà specifiche dell'area geografica di applicazione [66] . Sinteticamente tutte queste caratteristiche possono essere sinteticamente fatte rientrare nel requisito della c.d. *data quality*.

L'importanza della qualità dei dati è fondamentale. Diversi rischi sono direttamente connessi all'utilizzo di dati scadenti o incorretti per addestrare algoritmi *machine learning* non supervisionati in quanto, dati di addestramento oggettivamente errati portano a previsioni errate[67] che possono comportare anche delle conseguenze gravi nella sfera giuridica degli individui[68].

Attualmente, nell'ordinamento europeo vi sono già delle previsioni che eviterebbero le criticità relative alla qualità dei dati, i quali potrebbero, nel frattempo, agire in luogo dell'art. 10 AIA. In particolare, la soluzione principale è riscontrabile proprio nel GDPR. L'addestramento dei sistemi di IA, infatti, si basa sulla raccolta di dati

[65] Ai sensi dell'art. 3, n. 3 AIA il fornitore è "*una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o che fa sviluppare un sistema di IA al fine di immetterlo sul mercato o metterlo in servizio con il proprio nome o marchio, a titolo oneroso o gratuito*".

[66] Inoltre, le pratiche di governance e gestione dei dati devono riguardare: "*a) le scelte progettuali pertinenti; b) la raccolta dei dati; c) le operazioni di trattamento pertinenti ai fini della preparazione dei dati, quali annotazione, etichettatura, pulizia, arricchimento e aggregazione; d) la formulazione di ipotesi pertinenti, in particolare per quanto riguarda le informazioni che si presume che i dati misurino e rappresentino; e) una valutazione preliminare della disponibilità, della quantità e dell'adeguatezza dei set di dati necessari; f) un esame atto a valutare le possibili distorsioni; g) l'individuazione di eventuali lacune o carenze nei dati e il modo in cui tali lacune e carenze possono essere colmate.*"

[67] Sul punto, nel linguaggio colloquiale, si utilizza l'espressione "*garbage in – garbage out*" per evidenziare il fatto che l'immissione di dati di scarsa qualità porta inevitabilmente ad un *output* inaffidabile ed errato. Per approfondire v. T. ROSE, K. FISCHER, *Garbage In, Garbage Out: Having Useful Data Is Everything*, in *Measurement*, 9, 2011, 222-226, in Rete: *https://www.researchgate.net/publication/228449705_Garbage_In_Garbage_Out_Having_Useful_Data_Is_Everything*.

[68] La scorrettezza, in senso lato, dei dati di addestramento è, inoltre, la maggiore causa della discriminazione algoritmica. Tale fenomeno, infatti, accade ove i dati di addestramento non siano adeguatamente rappresentativi, ma siano invece negativamente influenzati da pregiudizi verso un particolare gruppo protetto. Anche se la qualità dei dati è la stessa per quanto riguarda i diversi gruppi protetti, la mancanza di equilibrio in un data set (ad esempio, la sottorappresentazione di un gruppo protetto, la cosiddetta distorsione del campionamento) può portare a distorsioni sistematiche e discriminazioni. Cfr. P. HACKER, *A Legal Framework for AI Training Data - From First Principles to the Artificial Intelligence Act*, in *Law, Innovation and Technology*, 2021, 3, in Rete: *https://ssrn.com/abstract=3556598*.

personali[69], ossia di un trattamento; pertanto, a questo dovranno essere applicati i principi e le garanzie previsti e, precisamente, il principio di accuratezza stabilito dall'art. 5, par. 1, lett. d) GDPR il quale prevede che "*i dati personali siano esatti e, se necessario, aggiornati*"[70]. Il suesposto articolo, tuttavia, non precisa in che misura i dati personali trattati debbano essere esatti e accurati, prevedendo solamente che il titolare del trattamento adotti "*tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati*". In tal senso, quindi, sarebbe rimesso al titolare determinare in che misura verificare l'esattezza dei dati personali, rischiando, conseguentemente, che, in caso di assenza di controllo sui dati di addestramento, il sistema di IA possa essere fondato su dati errati e che, quindi, possa assumere decisioni errate e potenzialmente lesive degli interessati[71].

Chiaramente, in tale circostanza entrerebbe in gioco il principio di *accountability* previsto dall'art. 5, par. 2 GDPR per mitigare tale rischio e gli eventuali trattamenti compiuti per la raccolta dei dati inesatti e l'addestramento dell'IA mediante gli stessi sarebbero illeciti, e potenzialmente sanzionabili ai sensi dell'art. 83 GDPR. Cionondimeno, è ragionevole ipotizzare che, rispetto a questo contesto, possa ben essere istituito un meccanismo di certificazione ai sensi del GDPR, il quale concentri i propri criteri di certificazione nella predisposizione di misure tecniche ed organizzative rivolte ad assicurare l'esattezza dei dati personali raccolti per l'addestramento di IA. D'altronde, proprio per il fatto di riuscire a adattarsi efficacemente alle evoluzioni tecniche e alle migliori prassi, lo strumento certificativo, al pari dei codici di condotta, potrebbe adeguatamente rappresentare la migliore soluzione per attestare la conformità al requisito di esattezza dei dati non solo ai sensi del GDPR, ma anche in tutte le declinazioni previste dall'art. 10 dell'AIA e riferite alla *data quality*[72], ossia pertinenza, rappresentatività, esattezza, completezza e che tenga conto del fattore della diversità dei gruppi sociali[73].

---

[69] Rimane il fatto che potrebbero anche essere utilizzati dati anonimizzati, i quali sono esclusi dall'ambito applicativo del Reg. (UE) 2016/679. Tuttavia, come si è precedentemente indicato, l'anonimità di un dato è garantita dalla capacità di altri dispositivi di deanonimizzarlo mediante informazioni aggiuntive che permettano di identificare nuovamente l'interessato. Perciò, anche dati apparentemente anonimi potrebbero essere considerati dati personali ai sensi del GDPR.

[70] In questo modo, dato che gli interessati dovrebbero essere sempre informati dell'utilizzo dei loro dati ai fini dell'apprendimento di un IA, questi potrebbero direttamente intervenire per chiedere la rettifica o la cancellazione dei propri dati ai sensi degli artt. 16 e 17 GDPR, in modo da non subire conseguenze pregiudizievoli per le decisioni algoritmiche errate.

[71] A fronte di ciò, quindi, dovrebbero attivarsi meccanismi risarcitori volti a ristorare l'eventuale utente-interessato leso da una decisione algoritmica scorretta. Sul punto, per approfondire, si segnala la recente proposta di Direttiva del Parlamento Europeo e del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (direttiva sulla responsabilità da intelligenza artificiale), in Rete: *https://eur-lex.europa.eu/legal-content/it/txt/?uri=celex%3a52022pc0496*.

[72] Su questo punto si sottolinea che l'organismo internazionale di standardizzazione ha già previsto delle regole tecniche per assicurare la qualità dei dati con la certificazione ISO/IEC 25012. V. ISO, *ISO/IEC 25012*, in Rete: *https://iso25000.com/index.php/en/iso-25000-standards/iso-25012*.

[73] Per approfondire ulteriormente le caratteristiche di questi requisiti v. P. HACKER, *A Legal Framework for AI Training Data - From First Principles to the Artificial Intelli-gence Act*, *op. cit.*, 21-24.

CAPITOLO V - LE CERTIFICAZIONI PRIVACY: UN'ANALISI COMPARATA

1 Introduzione all'analisi comparata delle certificazioni privacy e data protection

In questo capitolo si intende analizzare le principali soluzioni sviluppate nei Paesi terzi all'Unione europea in merito ai meccanismi di certificazione per la protezione dei dati personali o per la privacy in generale.

La necessità di questo approfondimento è dettata principalmente dal fatto che ormai la globalizzazione e lo sviluppo delle tecnologie hanno reso il commercio, non solo materiale, ma dei dati e delle informazioni, di portata globale, scollegata ai confini territoriali o giuridici stabiliti dalle norme eurocomunitarie. Proprio per tale ragione non è stata privilegiata l'analisi delle sole certificazioni strettamente collegate alla protezione dei dati personali ma anche quelle relative, in senso lato, alla privacy. Infatti, al di fuori del continente europeo, difficilmente si riscontrano testi legislativi specifici e completi come il GDPR, con la conseguenza che gli strumenti di autoregolamentazione o di co-regolamentazione saranno necessariamente di maglie più larghe rispetto agli artt. 42 e 43 del Regolamento.

Nonostante ciò, si è scelto di approfondire gli ordinamenti giuridici che, per ragioni comuni, sono i più connessi, se non influenzati, con la normativa europea, ossia Regno Unito, Canada e Stati Uniti.

Partendo dal Regno Unito, il panorama certificativo di quest'ultimo è stato prescelto in quanto lo stesso faceva ancora parte dell'Unione europea quando è stato promulgato ed è entrato in vigore il GDPR. Inoltre, la normativa interna e le tutele connesse alla protezione dei dati personali sono state comunque sviluppate sull'influsso della Direttiva Madre, determinando una ragguardevole somiglianza tra la normativa europea e quella britannica. Ciò consente di ritenere ragionevolmente che anche i possibili strumenti auto e co-regolativi possano somigliare ai codici di condotta e alle certificazioni previste ai sensi del GDPR.

Con riguardo al Canada, oltre il fatto che il suo ordinamento giuridico si pone a metà tra il *civil law* europeo e il *common law* anglo-americano, è comunque il Paese che ha visto nascere il concetto della *privacy by design*, tramutato, poi, nella *data protection by design* e *by default*. Proprio lo sviluppo di tali principi e la loro interpretazione in relazione alla disciplina interna sulla protezione dei dati personali, potrebbe costituire il substrato necessario per consentire lo sviluppo di certificazioni strettamente rivolte alla protezione dei dati personali e non delle semplici certificazioni privacy.

Infine, è stato vagliato l'ecosistema statunitense sulle certificazioni in quanto rappresenta il mercato più rilevante per le nuove tecnologie e, di conseguenza, uno fra i principali Paesi terzi con cui l'UE trattiene relazioni commerciali. Come si avrà modo di spiegare successivamente, negli Stati Uniti non è presente una disposizione legislativa unitaria sulla protezione dei dati personali in ragione dell'iniziale disinteresse alla *data protection*. Ciò ha direttamente influito sullo sviluppo di strumenti autoregolativi i quanti sono principalmente rivolti alla tutela, in senso lato, della privacy. Solo i vari trattati stipulati con l'UE per il trasferimento transfrontaliero di dati personali, con le

connesse decisioni di adeguatezza della Commissione, hanno contribuito direttamente allo sviluppo di meccanismi certificativi rivolti alla protezione dei dati personali, ma principalmente per garantire l'adeguatezza con l'UE.

2 Regno Unito: UK-GDPR e i primi schemi di certificazione approvati

A partire dalla Brexit il Regno Unito ha messo in costante discussione l'applicazione del GDPR all'interno del Paese. Pur non essendo più un Paese membro nel 2019 è stato firmato dal Regno Unito l'Accordo sul recesso del Regno Unito di Gran Bretagna e Irlanda del Nord dall'Unione europea e dalla Comunità europea dell'energia atomica all'interno del quale, al paragrafo 1 dell'art. 71, veniva previsto che: "*Il diritto dell'Unione in materia di protezione dei dati personali si applica nel Regno Unito al trattamento dei dati personali degli interessati al di fuori del Regno Unito, purché tali dati personali: a) siano stati trattati nel Regno Unito ai sensi del diritto dell'Unione prima della fine del periodo di transizione; o b) siano trattati nel Regno Unito dopo la fine del periodo di transizione in virtù del presente accordo*". Di fatti per il c.d. periodo di transizione nel Regno Unito si sarebbe comunque applicato il GDPR, determinando l'ultrattività delle regole, obblighi e principi ivi previsti, fra cui le norme relative ai codici di condotta e ai meccanismi di certificazione.

Solo a partire dal 1° gennaio 2021 il Regno Unito si sarebbe definitivamente distaccato dalla normativa europea a protezione dei dati personali, rimanendo, però, indelebilmente condizionato nella previsione di una normativa nazionale corrispondente a quella europea. L'influenza determinata dall'originaria applicazione del Regolamento (UE) 2016/679, infatti, aveva determinato la creazione di una normativa organica in materia di protezione dei dati, ossia il *Data Protection Act* 2018, che, successivamente alla Brexit, è stato emendato con il c.d. UK-GDPR. Nonostante le modifiche normative, la disciplina sulla protezione dei dati personali nel Regno Unito risulta sostanzialmente identica a quella del Regolamento europeo, tant'è che le principali norme relative ai principi per la protezione dei dati personali, nonché gli obblighi di *accountability* principali sono rimaste sostanzialmente identiche, salvo modifiche di sistema relative alla rimozione delle istituzioni europee.

Al medesimo processo di revisione sono stati sottoposti anche gli articoli del GDPR relativi ai meccanismi di certificazione, ora disciplinati all'art. 17 del DPA e di un allegato specifico[1]. In particolare, possono assegnare certificazioni ai sensi del UK-GDPR gli Organismi di Certificazione che siano stati accreditati dall'UKAS[2] sulla base di un meccanismo di certificazione i cui criteri siano stati approvati dall'ICO.

Come nel Regolamento europeo, il DPA non disciplina compiutamente i meccanismi di certificazione, rimettendo la definizione della procedura di creazione dei criteri di certificazione e della metodologia di valutazione all'ICO e all'UKAS. In particolare, è proprio nelle linee guida pubblicate dall'Autorità inglese che si evince

[1] Cfr. Data Protection Act 2018, §17 e Schedule 5 — Accreditation of certification providers: reviews and appeals, in Rete: *https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf*.

[2] L'UKAS è organismo nazionale di accreditamento del Regno Unito istituito dal governo per valutare la competenza delle organizzazioni che forniscono servizi di certificazione, test, ispezione e calibrazione. In Rete: *https://www.ukas.com/*.

l'oggetto delle certificazioni ai sensi dell'UK-GDPR: queste ultime devono riguardare una specifica operazione di trattamento o un insieme di trattamenti che costituiscono un prodotto, processo o servizio offerto dall'organizzazione che intende certificarsi[3]. Rispetti, poi, ai singoli trattamenti svolti dal soggetto richiedente la certificazione, quest'ultimo dovrà individuare, sulla base dei criteri forniti dalle varie certificazioni, il ToE rispetto al quale sottoporre a valutazione i trattamenti per il conseguimento della certificazione.

Scopo delle certificazioni, anche nel UK-GDPR, è quello di dimostrare il rispetto degli obblighi di accountability e la conformità di uno specifico trattamento alle norme a protezione dei dati personali. Da ciò, incoraggiando e premiando la conformità dei soggetti certificati, ai meccanismi di certificazione viene assegnato un valore probatorio importante, utile a dimostrare all'ICO, oltre che ai terzi, la conformità alle norme del *Data Protection Act*[4]. A tal fine, in caso di *incident* comportati una violazione dei dati personali, gli schemi di certificazione potranno essere eventualmente valutati come un fattore attenuante in caso di indagini ed ispezioni del Garante inglese. Proprio per la loro valenza probatoria, queste permetterebbero di dimostrare l'adozione da parte del soggetto certificato di tutte le misure adeguate e ragionevoli per assicurare la protezione e la sicurezza dei dati personali trattati, nonché i diritti e le libertà degli interessati. Pertanto, in caso di violazioni è ragionevole aspettarsi che la certificazione venga valutata come un fattore attenuante rispetto alla possibile sanzione irrogabile. Tuttavia, non sempre la certificazione può avere tale valenza; come precedentemente illustrato, infatti, in caso di gravi violazioni determinati dalla mancata osservanza delle norme del DPA e dei criteri di certificazione, l'adesione ad uno schema potrà essere valutato dall'ICO come un'aggravante, in ragione della gravità della violazione[5].

Il processo per la creazione di uno schema di certificazione inizia con lo sviluppo e l'approvazione dei relativi criteri di certificazione. Come specificato dall'ICO, i criteri di certificazioni devono concentrarsi sull'approfondita valutazione degli specifici trattamenti che vengono effettuati e di come i dati vengono trattati[6]. I criteri di certificazione dorano necessariamente essere tratti dalla normativa inglese sulla protezione dei dati personali, ma potranno comunque avere una portata applicativa generica, concernente tutti gli aspetti del UK-GDPR, o specifica, rispetto ad un determinato settore o ad una tipologia specifica di trattamenti[7]. Importante, inoltre, è l'interoperabilità dei criteri rispetto ad altre norme tecniche e, soprattutto, la scalabilità

[3] Come nel GDPR europeo, quindi, la certificazione può avere ad oggetto uno, una parte o più trattamenti di dati personali che costituiscono un unitario prodotto, processo o servizio.

[4] Cfr. IMPACT NEWS SERVICE, *New certification schemes will "raise the bar" of data protection in children's privacy, age assurance and asset disposal*, in *LexisNexis*, 2021, in Rete: *https://advance.lexis.com/api/document?collection=news&id=urn:contentitem:63f7-2yd1-jdg9-y46w-00000-00&context=1516831*.

[5] Cfr. ICO, *Will the ICO consider certification as a mitigating factor in an investigation?*, in Rete: *https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-schemes-detailed-guidance/how-do-we-apply-for-gdpr-certification/#how5*.

[6] Da questo punto di vista, l'ICO sottolinea che più che concentrarsi sulla disposizione di *governance* e sulla gestione dei dati trattati, bisogna analizzare attentamene le specifiche tecniche e misure adottate dai titolari e responsabili del trattamento che intendono aderire alla certificazione.

[7] Sul punto l'ICO elenca alcuni elementi che lo *scheme owner* deve tenere in considerazione per decidere l'ambito di applicazione della certificazione.

della certificazione rispetto alle diverse dimensioni delle organizzazioni che intendono certificarsi. A differenza del UE-GDPR, le certificazioni privacy nel Regno Unito devono soddisfare un ulteriore requisito, ossia devono essere capaci di soddisfare un'identificata necessità od esigenza nel settore della protezione dei dati personali. Secondo l'ICO le certificazioni, in generale, devono avere uno scopo chiaro e devono coprire un'ampia gamma di attività di trattamento diverse, in modo da poter soddisfare le esigenze sulla protezione dei dati personali richieste dal mercato o dai consumatori (interessati)[8].

L'ICO non è l'unico ente protagonista del procedimento di approvazione della certificazione. Quest'ultima, infatti, ha lo specifico ruolo di asservare i criteri di certificazione dello schema ma, in seguito, per la completa convalida è necessario l'intervento dell'UKAS. Per l'esattezza, il coinvolgimento dell'organismo nazionale di accreditamento inglese è necessario per valutare le metodologie di *audit* e i modelli di controllo previsti dallo schema per gli OdC al fine di verificare la conformità dei soggetti che intendono certificarsi[9]. In particolare, le metodologie di valutazione dovranno considerare l'ambito di applicazione dello schema e i potenziali (o comunque i più frequenti) trattamenti suscettibili di certificazione.

Infine, l'ICO, oltre ad approvare i criteri di certificazione dei singoli schemi, ha il compito di monitorare il costante rispetto delle norme poste a presidio della procedura certificativa, oltre che della normativa sulla protezione dei dati personali. L'intervento dell'Autorità del UK può essere talmente pervasivo che durante il processo di certificazione, l'OdC è tenuto a comunicare all'autorità le credenziali del soggetto che intende certificarsi e se quest'ultimo è sottoposto ad un procedimento di ispezione, ciò rappresenta una ragione ostativa al rilascio della certificazione.

Come nel Regolamento europeo sulla protezione dei dati, le certificazioni vengono attribuite da Organismi di Certificazione appositamente accreditati dall'UKAS. Come si è visto, gli OdC possono corrispondere o meno con gli *scheme owner*; tale circostanza determina una parziale differenziazione del procedimento di accreditamento in quanto, se un OdC è titolare anche di un proprio meccanismo di certificazione questo dovrà essere approvato dall'ICO e successivamente potrà essere accreditata dall'UKAS. Nel caso inverso, invece, l'OdC sarà solamente accreditato dall'organismo nazionale di accreditamento del Regno Unito, rispetto ad una determinata certificazione, sulla base

[8] Tali elementi dovranno essere necessariamente provati nella domanda per l'approvazione dei criteri di certificazione. In particolare, lo *scheme owner*, oltre ad evidenziare i vantaggi per i titolari o responsabili del trattamento e per gli interessati devono: dar prova del fatto che la propria certificazione soddisfi una determinata esigenza o necessità del settore della protezione dei dati personali; dar prova del valore aggiunto della propria certificazione rispetto a schemi già esistenti; evidenziare i settori economici, sociali, tecnologici, legali o di altro tipo rilevanti che possono essere influenzati dalla certificazione e del suo sviluppo e applicazione; dimostrare, infine, che i criteri di certificazione si fondano su priorità legislative, governative, individuate dall'ICO o provenienti dal mercato e dagli interessati al trattamento. Tali elementi saranno specificatamente valutati dall'ICO secondo attraverso i controlli individuati nelle linee guida per l'approvazione dei criteri di certificazione. Cfr. ICO, *How do we develop a certification scheme?*, in Rete: *https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-schemes-detailed-guidance/how-do-we-develop-a-certification-scheme/#10*.

[9] La frammentazione del procedimento di approvazione della certificazione fra le due autorità permette agli *scheme owner* di realizzare alternativamente anche solo i criteri, che verranno approvati singolarmente dall'ICO, o uno schema completo anche della metodologia di valutazione.

delle eventuali indicazioni fornite dallo *scheme owner*. In ogni caso, l'accreditamento degli OdC avviene sulla base del rispetto delle norme tecniche contenute nella ISO/IEC 17065 e ai requisiti di accreditamento aggiuntivi stabiliti dall'ICO, come nell'UE. Ovviamente, l'OdC per essere accreditato deve garantire la propria terzietà, imparzialità e indipendenza rispetto a soggetti terzi e, in particolare, alle organizzazioni richiedenti la certificazione. L'OdC deve, inoltre, dimostrare la propria conformità al UK-GDPR e la specifica competenza del proprio personale rispetto alla materia della protezione dei dati personali[10]. Una volta accreditati al rilascio di un meccanismo di certificazione gli OdC saranno chiamati a monitorare la costante conformità dei soggetti certificati e a provvedere alla sospensione o revoca della certificazione nel caso in cui questi ultimi non soddisfino più i criteri di certificazione.

A fronte di questo contesto, alquanto simile a quello europeo, il mercato delle certificazioni sulla protezione dei dati personali ha avuto uno sviluppo più rapido nel Regno Unito rispetto al continente europeo. Attualmente l'ICO ha, infatti, approvato quattro meccanismi di certificazione:

1. Age Check Certification Scheme (ACCS): lo *scheme owner* Age Check Certification Scheme ha sviluppato due meccanismi di certificazione rivolti, il primo (ACCS), alla verifica dei trattamenti che consentono di stimare e verificare l'età di una persona (in modo da imporre dei limiti di età all'accesso dei prodotti o servizi certificati)[11] e, il secondo (AADCS), alla verifica della corretta implementazione del principio della *privacy by design* per i prodotti o servizi destinati ai minori. Entrambi gli schemi hanno l'obiettivo principale di verificare la conformità di un'organizzazione agli obblighi in tema di verifica dell'età e di trattamenti dei dati dei minorenni e, pertanto, di rispondere alle esigenze pubbliche relative alla tutela della privacy dei bambini. Per tale ragione, l'ambito applicativo della certificazione è molto ristretto, concernendo il rispetto di tutti gli obblighi di *accountability* relativi ai trattamenti di dati personali per la verifica dell'età[12]. I criteri di certificazione dell'ACCS intendono fornire una serie di criteri tecnici volti a valutare l'efficacia e l'accuratezza dei trattamenti di controllo dell'età dei clienti e l'appropriata

[10] Per delle indicazioni più esaustive, però, l'ICO fa direttamente riferimento alle Linee Guida 4/2018 dell'EDPB, nonostante non siano più direttamente applicabili al Regno Unito.

[11] Cfr. ICO, *Certification schemes register: Age Check Certification Scheme (ACCS)*, 2021, in Rete: *https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-scheme-register/age-check-certification-scheme-accs/*.

[12] Nell'evidenziare lo scopo dello schema di certificazione, i criteri di certificazione ACCS 2-2021 ricomprendono i trattamenti svolti da titolari e co-titolari del trattamenti in servizi di: "*a) Proof-of-Age ID Providers that verify age attributes and issue a reusable physical ID card, token or app that an unknown third party (such as a retailer) can rely on with or without a pre-arranged contractual relationship with the Proof-of-Age ID Provider; b) Age Check Providers that verify age attributes on request by a third party on a transaction-by-transaction basis under a pre-arranged contractual relationship with the Age Check Provider; c) Age Check Exchange Providers or Brokers that provide an online gateway for Age Check Providers and Relying Parties to access user asserted, permissioned and verified attributes; d) Relying Parties (online or offline) that rely on results of an age check (either remotely or during a face-to-face encounter) to establish the age-related eligibility of an individual for the purposes of a transaction (such as sellers or providers of age restricted goods and services)*". Cfr. AGE CHECK CERTIFICATION SCHEME LTD, *ACCS 2:2021 Technical Requirements for Data Protection and Privacy*, 2021, 5-8, in Rete: *https://ico.org.uk/media/for-organisations/documents/2620426/accs-2-2021-technical-requirements-aadc.pdf*.

progettazione di questi sistemi[13]. In particolare, il marchio di certificazione sarà attribuito all'organizzazione richiedente solamente ove siano positivamente soddisfatti una serie di controlli relativi ai diversi sistemi di verifica dell'età, fra cui, ad esempio: il funzionamento efficacie degli strumenti di verifica basati su video-identificazione in diverse condizioni di illuminazione ed ambientali; il funzionamento della verifica dei documenti di identità; il funzionamento dei sistemi di *social proofing*, ossia di conferma dell'età tramite un ulteriore richiesta di convalida a contatti terzi verificati (come genitori e/o altri terzi); il funzionamento degli strumenti di verifica biometrici; di verificare, infine, l'acquisizione del consenso dei genitori una volta accertata la minore età dell'interessato.

2. Age Appropriate Design Certification Scheme (AADCS), il secondo meccanismo di certificazione realizzato dall'ACCS intende fornire, come anticipato, una serie di criteri per la progettazione adeguata dei servizi di verifica dell'età, nel rispetto del principio della DPbDD e dei principi del Children's Code britannico. Rispetto all'ambito applicativo soggettivo, lo schema AADCS risulta più generico rispetto al ACCS; viene previsto che la certificazione possa essere applicata ad ogni trattamento relativo a servizi forniti dalle 'società dell'informazione' che risultano accessibili ai minori nel Regno Unito[14]. Infine, con riguardo all'ambito oggettivo, lo schema AADCS fornisce, come detto, tutta una serie di requisiti tecnici, organizzativi e documentali che le organizzazioni operanti nel trattamento dei dati personali dei minori devono avere per dimostrare la propria conformità al Children's Code. I criteri di certificazione si dividono in 15 sezioni concernenti: a) il perseguimento del miglior interesse del bambino; b) lo svolgimento di una valutazione d'impatto per la protezione dei dati personali; (c) l'adozione di un approccio basato sul rischio per la verifica dei sistemi di controllo dell'età; (d) la trasparenza nel trattamento dei dati; (e) la prevenzione contro l'uso dannoso dei dati; (f) *policies* e regolamenti aziendali; (g) la protezione dei dati per impostazione predefinita (*data protection by default*); (h) La minimizzazione dei dati trattati; i) l'implementazione di misure di limitazione della condivisione e trasmissione dei dati del minore; (j) la stigmatizzazione dei sistemi di geolocalizzazione[15]; (k) i meccanismi di *parental controls* e la relativa informativa da fornire al minore; (l) la stigmatizzazione della profilazione[16]; (m) la proibizione di tecniche di *nudging* ; (n)

[13] Oltre a verificare la corretta implementazione delle misure tecniche ed organizzative necessarie a garantire la liceità dei trattamenti di verifica dell'età. Per approfondire v. *ivi*, 20-66.

[14] Con riguardo a tale definizione è da ritenersi che la certificazione sia applicabile sia ai titolari e co-titolari del trattamento, che ai responsabili del trattamento.

[15] I quali vengono comunque consentiti in caso di necessità che siano comunque nel miglior interesse del minore (tutela della salute, sicurezza, integrità fisica e morale). Cfr. AGE CHECK CERTIFICATION SCHEME LTD, *ACCS 3:2021 Technical Requirements for Age Appropriate Design for Information Society Services*, 2021, 36, in Rete: *https://ico.org.uk/media/for-organisations/documents/2620427/accs-3-2021-technical-requirements-aadc.pdf*; ICO, *Certification scheme register: Age Appropriate Design Certification Scheme (AADCS)*, 2021, in Rete: *https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-scheme-register/age-appropriate-design-certification-scheme-aadcs/*.

[16] I criteri sono chiari nel prevedere che per *default* la profilazione e i trattamenti automatizzati dei dati del minore non possano essere effettuati se non in particolari eccezioni. In ogni caso in cui fosse consentita

l'estensione dei criteri di certificazione anche a giocattoli o altri dispositivi interconnessi; (o) la previsione di strumenti adeguati per consentire al minore l'esercizio dei propri diritti nonché per segnalare possibili illiceità.

3. ICT Asset Recovery Standard 8.0: l'ADISA, quale *scheme owner* dello schema, ha sviluppato un meccanismo di certificazione che si occupa di garantire che i dati personali siano trattati correttamente al momento dello smaltimento delle risorse e apparecchiature informatiche[17]. La certificazione disciplina compiutamente il processo di smaltimento individuando procedure e modalità operative basate sul rischio per le attività di trattamento basate sulla 'sanificazione' dei supporti di memorizzazione dai dati personali[18]. Il fatto che i criteri di certificazione siano sviluppati sulla base del *risk-based approach* determina che le misure da implementare e i controlli per la valutazione della conformità del soggetto richiedente la certificazione divergano in relazione alle diverse categorie dei dati trattati; il trattamento di categorie particolari di dati o di dati relativi a condanne penali, quindi, sono sottoposti a controllo più rigidi rispetto agli altri trattamenti di dati personali 'ordinari'. L'ambito soggettivo della certificazione coinvolge sia i titolari del trattamento (e co-titolari), sia responsabili e *sub*-responsabili del trattamento. Con riguardo, infine, ai criteri di certificazione, questi sono allineati alle norme del UK-GDPR, pretendendo il rispetto dei relativi principi ed obblighi con una focalizzazione ad alto livello al trattamento di smaltimento sicuro dei dati[19].
4. UK GDPR Compliance Certification Scheme for the Provision of Training and Qualifications Services[20], sviluppato da APMG, ha l'obiettivo di promuovere la

---

la profilazione, comunque, il titolare del trattamento dovrà adottare tutte quelle misure necessarie per proteggere il minore da ogni effetto dannoso.

[17] Le diverse operazioni incluse nell'ambito oggettivo di applicazione includono il coinvolgimento dei clienti, i servizi logistici, lo stoccaggio, la gestione delle risorse e il riciclaggio o la rivendita di apparecchiature ICT. Cfr. ADISA CERTIFICATION LTD, *ICT Asset Recovery Standard 8.0 Part 1: Introduction and Explanatory Notes*, 2022, 3, in Rete: *https://ico.org.uk/media/for-organisations/documents/4021012/adisa-asset-recovery-standard-8_0-v3_1-part-1-introduction-and-explanation-notes.pdf*; ICO, *Certification scheme register: ADISA ICT Asset Recovery Certification 8.0*, 2021, in Rete: *https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-scheme-register/adisa-ict-asset-recovery-certification-80/*.

[18] Il trattamento consistente nella 'sanificazione dei dati' si riferisce al processo di distruzione permanente e irreversibile dei dati su un dispositivo di memorizzazione, il quale può avvenire alla conclusione del periodo di vita del dispositivo, a conclusione del noleggio del dispositivo o in sede di manutenzione di dispositivi non funzionati di memorizzazione dei dati per finalità di recupero del dispositivo medesimo, il quale però non è destinato ad essere restituito al titolare del trattamento (es. prodotti ricondizionati nuovamente venduti al pubblico). Cfr. ADISA CERTIFICATION LTD, *ICT Asset Recovery Standard 8.0 Part 1: Introduction and Explanatory Notes*, *op. cit.*, 4.

[19] Cfr. *ivi*, 10 e ss. Una particolarità dello schema di certificazione è la previsione di un nuovo documento di verifica del rischio distinto dalla DPIA. Infatti, per garantire che il titolare del trattamento possa controllare il proprio rischio senza essere determinato dal solo costo, viene introdotto il *Data Impact Assurance Levels* (DIAL), mediante il quale valutare il rischio del trattamento di sanificazione sulla base di 5 variabili, ossia: 1. Minacce; 2. Propensione al rischio; 3. Categoria di dati; 4. Volume di dati; 5. Impatto di una violazione dei dati.

[20] Cfr. THE APM GROUP LTD (APMG), *UK GDPR Compliance Certification Scheme for the Provision of Training and Qualifications Services Criteria*, 2022, in Rete: *https://ico.org.uk/media/for-organisations/documents/4023361/uk-gdpr-compliance-certification-scheme-for-the-provision-of-*

fiducia nelle società della formazione delle risorse umane che trattano dati personali. Consente agli interessati di fare una scelta informata nel selezionamento delle imprese attive nella formazione professionale ed essere sicuri che i loro dati personali saranno trattati in conformità con il UK-GDPR. I criteri si applicano al trattamento dei dati personali da parte delle società di formazione (private e pubbliche), che agiscono in qualità di responsabili del trattamento, in tutte le attività relative alla loro fornitura di servizi di formazione e qualifiche a candidati di età superiore ai 16 anni. Questo schema di certificazione è stato elaborato con l'obiettivo di promuovere la fiducia nei centri di formazione che trattano dati personali. Le imprese di formazione certificate riceveranno un marchio/sigillo per dimostrare che le loro attività di elaborazione, in relazione ai loro servizi di formazione e qualifiche, sono conformi ai requisiti dello schema di certificazione, consentendo agli interessati di fare una scelta informata quando selezionano una società di formazione e possono essere sicuri che i loro dati personali saranno trattati in conformità con il GDPR del Regno Unito. Questa certificazione copre le attività delle società di formazione il cui lavoro può includere la fornitura di servizi di formazione e qualifiche agli individui e la successiva comunicazione dei risultati di tali attività, la commercializzazione agli individui, la segnalazione agli Organismi di Certificazione e, quando richiesto, alle autorità. Lo schema si applica all'intero ciclo di vita dei dati, vale a dire a tutte le fasi del trattamento dei dati personali relativi all'erogazione della formazione e delle qualifiche. Ciò vale per tutti i dati personali trattati, compresi quelli appartenenti a terzi, quando si forniscono questi servizi. Gli unici trattamenti esclusi, in quanto non rilevanti per le finalità di formazione e qualifica, sono quelli relativi ai minori di 16 anni e i dati personali concernenti condanne penali e reati. L'impresa di formazione specifica le attività di trattamento soggette a certificazione (obiettivo della valutazione), tenendo conto delle attività di trattamento coinvolte nella fornitura di servizi di formazione e qualifiche da un capo all'altro (ciclo di vita). Queste devono inoltre fornire una mappa dei trattamenti, il quale identifichi tutti i sistemi e i software usare; gli strumenti di hosting, i responsabili del trattamento coinvolti, i destinatari dei trasferimenti dei dati personali e il periodo di conservazione dei dati, identificando, altresì, eventuali categorie particolari di dati trattate. Rispetto a questi trattamenti lo schema si occupa di verificare il rispetto dei requisiti generali e dei principi del UK-GDPR[21], il rispetto delle condizioni per un libero consenso, le modalità di gestione delle istanze di esercizio dei diritti degli interessati, la formulazione di

training-and-qualifications-services-v-6_2.pdf; ICO, *Certification scheme register: Provision of Training and Qualifications Services*, in Rete: *https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-scheme-register/provision-of-training-and-qualifications-services/*.

[21] Quali, ad esempio, la nomina del DPO, la formazione del personale, le verifiche di *audit*, il rispetto della DPbDD, lo svolgimento di DPIA e la soddisfazione dei principi di liceità, correttezza e trasparenza; limitazione delle finalità; limitazione della conservazione; minimizzazione dei dati; accuratezza; integrità e riservatezza.

un'informativa chiara a questi ultimi ed altri requisiti operativi (segnalazioni *data breach*, Registro dei trattamenti, cooperazione con le autorità, ecc.)[22].

In conclusione, le certificazioni sulla protezione dei dati personali cominciano ad avere un intenso sviluppo anche nel Regno Unito nonostante l'uscita dall'Unione europea. Infatti, dopo le citate certificazioni l'ICO correntemente impegnata nel dialogo con altre organizzazioni per lo sviluppo di nuovi meccanismi di certificazione. D'altronde conformare il livello della protezione dei dati personali ad uno standard univoco a quello europeo permetterebbe agevolmente alle organizzazioni britanniche di mantenere un rapporto di conformità anche al GDPR, consentendo l'agevole scambio di dati personali UK-UE[23].

3 Canada: La Privacy by Design Certification Shield del Privacy and Big Data Institute of Ryerson University

Come già anticipato in precedenza, ad Ann Cavoukian si deve l'elaborazione dei principi della privacy by design e by default, i quali hanno indelebilmente influenzato l'ordinamento giuridico canadese, nonostante lo stesso non abbia una norma legislativa che ne codifichi il contenuto. In Canada, infatti, la protezione dei dati personali o, meglio, l'*informational privacy*, è garantita quale esplicazione delle *Section 7-8* del *Canadian Charter of Rights and Freedoms* come interpretate dalla giurisprudenza canadese[24]. Oltre a ciò, il diritto all'*informational privacy* è tutelato da una serie di norme legislative sia a livello federale, sia a livello delle singole province. A livello federale la legislazione principale sulla protezione dei dati personali nel settore privato è il *Personal Information Protection and Electronic Documents Act* (PIPEDA) del 2001[25]. Tale legge tutela le informazioni personali relative ad un individuo identificato[26], stabilendo i requisiti e i principi che i trattamenti devono rispettare per essere considerati leciti[27] e attribuendo agli interessati una serie di diritti simili a quelli del GDPR.

---

[22] Cfr. THE APM GROUP LTD (APMG), *UK GDPR Compliance Certification Scheme for the Provision of Training and Qualifications Services Criteria*, *op. cit.*, 12-36.

[23] In ogni caso, il trasferimento transfrontaliero di dati UK-UE si basa sulla Decisione di adeguatezza della Commissione europea n. 1772/2021. Cfr. COMMISSIONE EUROPEA, *Commission Implementing Regulation (EU) 2021/1772*, 2021, in Rete: *https://eur-lex.europa.eu/legal-content/en/txt/?uri=celex%3a32021d1772*.

[24] La Corte suprema canadese, infatti, con il caso R. v. Spenser del 2014 ha definitivamente chiarificato come nel principio di *informational privacy* rientri non solo la protezione della segretezza e riservatezza delle informazioni, ma anche il loro controllo, accesso e utilizzo. Cfr. P. GUARDA, G. BINCOLETTO, *Diritto comparato della privacy e della protezione dei dati personali*, *op. cit.*, 120.

[25] Cfr. M. BHASIN, *Challenge of Guarding Online Privacy: Role of Privacy Seals And Government Regulations*, in *South Asian Journal of Marketing & Management Research*, 3 (2), 2016, 69, in Rete: *https://www.researchgate.net/publication/309407924_challenge_of_guarding_online_privacy_role_of_privacy_seals_and_government_regulations*.

[26] A differenza del GDPR non si considerano, e quindi non sono tutelati, i dati personali relativi ad un soggetto non direttamente identificato ma comunque identificabile. La tutela per i dati relativi ad un soggetto individuabile è apprestata solamente nell'ipotesi in cui ci sia una seria possibilità che tramite altre informazioni l'interessato possa essere nuovamente individuato.

[27] Quali il principio di limitazione delle finalità, confidenzialità e sicurezza, limitazione della conservazione e *accountability*.

Il *Bruxelles Effect* provocato dal GDPR[28] ha comportato rilevanti cambiamenti anche nel sistema canadese. Infatti, negli ultimi anni sono stati diversi i tentativi di riforma delle leggi canadesi sulla privacy, contribuendo ad un cambiamento di prospettiva maggiormente organico e completo della protezione dei dati come diritto riconosciuto dall'ordinamento. Da ultimo, è di nota il *Bill C 27: Digital Charter Implementation Act 2022*, avente lo scopo di introdurre un nuovo testo legislativo che dovrebbe abrogare gran parte dei PIPEDA, ossia il *Consumer Privacy Protection Act*[29]. Con il nuovo progetto di legge saranno introdotti nuovi obblighi per il trattamento di dati personali, riconosciuti nuovi diritti agli interessati e verrà introdotto un nuovo organismo, il *Personal Information and Data Protection Tribunal,* per dirimere, in secondo grado rispetto alle decisioni dell'Autorità canadese di protezione dei dati, le controversie relative alla violazione della normativa a protezione dei dati personali.

Nel PIPEDA, come nel resto dell'attuale legislazione canadese, non si ha nessun riferimento a certificazioni o codici di condotta per la protezione dei dati personali. Tuttavia, già prima dell'entrata in vigore del PIPEDA si avvertiva la necessità per cui il Canada dovesse sforzarsi di costruire un ruolo quale attore globale nello sviluppo della politica di internet e della protezione dei dati. Il raggiungimento di tale obiettivo era determinato dall'opportunità di stabilire un marchio canadese di protezione dei dati dei consumatori riconosciuto a livello internazionale, il quale avrebbe dovuto essere sviluppato dal settore privato con la cooperazione del governo, dei gruppi di consumatori-interessati e dalla Canadian Standards Association (CSA) International[30]. Questo marchio sarebbe stato gestito da una terza parte neutrale incaricata di creare consapevolezza nei consumatori, promuovere l'adozione del programma di certificazione, monitorarne il rispetto e la conformità e fornire un sistema per la risoluzione delle controversie[31]. Proprio da questa visione, nonché dallo sviluppo internazionale dei principi della *privacy by design*, ha avuto genesi, nel 2015, il programma di certificazione Privacy by Design Certification Shield lanciato dal Privacy and Big Data Institute della Ryerson University.

Lo scopo dello schema di certificazione è quello di aiutare le aziende e le organizzazioni ad incorporare, in modo proattivo, la privacy nei propri processi sulla base del principio della *privacy by design*. Il programma di certificazione è supervisionato da un comitato consultivo presieduto da Ann Cavoukian ed è stato sviluppato in collaborazione con Deloitte Canada[32]. Quest'ultima, in particolare, ha avuto il ruolo di tradurre i sette principi della *privacy by design*[33] in 29 criteri misurabili empiricamente e

[28] Cfr. S. GUNST, F.DE VILLE, *The Brussels Effect: How the GDPR Conquered Silicon Valley*, in *European Foreign Affairs Review* 26, no. 3, 2021, 437–458, in Rete: *https://biblio.ugent.be/publication/8726790*.

[29] Cfr. GOVERNMENT OF CANADA, *Consumer Privacy Protection Act*, 2023, in Rete: *https://ised-isde.canada.ca/site/innovation-better-canada/en/consumer-privacy-protection-act*; P. GUARDA, G. BINCOLETTO, *Diritto comparato della privacy e della protezione dei dati personali*, *op. cit.*, 124.

[30] Proprio l'organismo nazionale di standardizzazione canadese ha sviluppato il codice di condotta per la protezione delle informazioni personali, che è il cuore della legislazione federale canadese sulla *privacy*.

[31] Cfr. A. CAVOUKIAN, M. CHIBBA, *Privacy Seals in the USA, Europe, Japan, Canada, India and Australia*, *op. cit.*, 76.

[32] Per approfondire v. Deloitte, *About Deloitte*, in Rete: *https://www2.deloitte.com/ca/en/pages/about-deloitte/articles/about-deloitte.html?icid=bottom_about-deloitte*.

[33] Cfr. *supra*, nota 68.

109 controlli illustrativi della privacy, tenendo conto dei requisiti chiave derivati dalle normative nazionali e internazionali sulla protezione delle informazioni personali e dalle *best-practices* maggiormente riconosciute[34].

Il campo applicativo della certificazione coinvolge la privacy nella progettazione, nel funzionamento e nella gestione di un determinato sistema informativo, processo aziendale o specifico progetto di rete. Da questo punto di vista, la Privacy by Design Certification Shield è molto simile alle certificazioni *data protection* previste ai sensi del GDPR, in quanto entrambe coinvolgono trattamenti di dati personali relativi a prodotti, processi o servizi[35]. Particolarità della certificazione canadese è la sua possibile applicazione internazionale. I criteri di certificazione della *privacy by design* individuati da Deloitte puntano, infatti, ad essere allineati al GDPR e alle altre normative principali internazionali sulla protezione dei dati personali, nonché alle normative di settore più importanti, come la certificazione ISO/IEC 27001[36].

Il processo inizia con la richiesta dell'organizzazione interessata alla certificazione. Il Privacy and Big Data Institute esamina la domanda e inoltra le informazioni a Deloitte per iniziare la valutazione. In questa fase il richiedente dovrà stipulare un accordo sia con la Ryerson University, disciplinante le obbligazioni del richiedente, i termini d'uso del marchio e le responsabilità per l'utilizzo dello stesso, sia con Deloitte, con riguardo agli obblighi di valutazione per la certificazione[37].

Successivamente Deloitte andrà a esaminare i prodotti, servizi e processi da certificare, conducendo interviste, analizzando la documentazione ed esaminando i trattamenti operativi. Deloitte pubblicherà quindi un *report* basato sulla metodologia di valutazione e sullo schema di valutazione sviluppato appositamente per i criteri della Privacy by Design Certification Shield per esamina l'aderenza dell'organizzazione ai criteri di certificazione[38].

---

[34] L'elenco dei criteri e le relative attività di controllo sono disponibili online. È importante notare il fatto che la certificazione *Privacy by Design*, pur essendo sviluppata dalla Ryerson University con il diretto coinvolgimento di Ann Cavoukian, non garantisce la diretta conformità rispetto alle leggi sulla *privacy* dell'Ontario.

[35] Cfr. EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, G. BODEA, K. STUURMAN, M. BREWCZYŃSKA, *Data protection certification mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679: annexes*, *op. cit.*, 65.

[36] È ragionevole pensare, quindi, che, se un'organizzazione straniera all'UE intendesse certificarsi con la *Privacy by Design Certification Shield* raggiungerebbe un livello di conformità significativo al GDPR rispetto ad altre possibili certificazioni *privacy*.

[37] Cfr. A. CAVOUKIAN, RYERSON UNIVERSITY, *Commit to Privacy, Publicly – Privacy by Design Certification Program*, in Rete: *https://www.torontomu.ca/content/dam/pbdce/certification/PbD-Brochure.pdf*, 6; RYERSON UNIVERSITY, *Privacy by Design Assessment and Certificatio*, in Rete: *https://www.torontomu.ca/content/dam/pbdce/certification/Privacy-by-Design-Overview_PbDCE.pdf*.

[38] In particolare, l'organizzazione che intende certificarsi dovrà essere conforme ai seguenti criteri di certificazione, individuate sulla base dei sette principi della *privacy by design*: "*• Privacy Governance-Responsibility and Accountability for Policies and Procedures • Privacy Impact Assessments or Privacy Risk Reviews • Privacy Incident and Breach Management • Compliance, Monitoring and Enforcement • Consistency of Privacy Policies and Procedures with Laws and Regulations • Privacy Training • Third Party Protection of Personal Information • Privacy Settings by Default • Data Minimization: Collection Limited to Identified Purpose • Use of Personal Information • Consideration of Privacy in Design Documentation • Privacy in Operational Procedures and Processes • Privacy in Change Management • Positive Sum (the organization can articulate and demonstrate the "positive sum" (e.g. no trade-offs; win/win)*

Sulla base dei risultati del *report* di Deloitte, il Privacy by Design Centre of Excellence si pronuncerà in merito all'attribuzione della certificazione o meno. In caso di esito positivo il Centro attribuirà il marchio denominato Certification Shield. Il marchio ha una durata massima triennale, soggetta a verifiche annuali di rinnovo per sorvegliare la costante conformità dell'organizzazione ai criteri di certificazione, nonché l'aggiornamento delle misure implementate per la protezione dei dati personali rispetto alle nuove tecnologie[39].

Oltre questo modello di 'rinnovo' annuale, non vi è nessun altro sistema di monitoraggio attivo per verificare la conformità delle organizzazioni certificate. Per sorvegliare la conformità il Privacy by Design Centre of Excellence si affida, difatti, solamente ad un meccanismo di segnalazione accessibile al pubblico tramite il proprio sito web, con il quale gli interessati possono dar conto delle eventuali violazioni o difformità del soggetto certificato. In tali occasioni, le ispezioni del Centro potranno portare anche alla sospensione o alla revoca della certificazione, quando riscontri o una violazione oggettiva delle condizioni stabilite nell'originario contratto di certificazione, un uso ultroneo del marchio di certificazione o il mancato allineamento delle tecniche ed organizzative richieste agli aggiornamenti dei principi o del programma di certificazione Privacy by Design Certification Shield[40].

Oltre a tali indicazioni, vi è infine da segnalare che non sono previsti per la certificazione degli organismi di certificazione, in quanto tutto il procedimento è gestito direttamente da Deloitte e dalla Ryerson University, mediante i rispettivi esperti.

A conclusione del processo di certificazione, l'organizzazione certificata sarà in grado di compiere un trattamento di dati personali tendenzialmente conforme alla normativa canadese, minimizzando i rischi derivanti da una possibile non-conformità. Questo, tuttavia, non rappresenta l'unico vantaggio. Lo sviluppo di una strategia *data protection* basata sulla Privacy by Design Certification Shield, permetterebbe di ridurre, di conseguenza, la probabilità di essere destinatari di sanzioni amministrative o penali, evitando perdite finanziarie derivanti da richieste di risarcimento per possibili violazioni

---

characteristics of the solution, product or service.) • Security in Privacy Policies • Safeguarding of Personal Information • Logical Access to Personal Information • Physical Access Controls • Environmental Safeguards • Transmitted Personal Information • Retention and Storage of Personal Information • Disposal, Destruction and Redaction of Personal Information • Testing Security Safeguards • Policies and Commitment • Openness • Purpose of Collection • Notice • Consent and Notice • Access to and Correction by Individuals of Their Personal Information • Right to deletion ("right to be forgotten") and right to object • Accuracy". Cfr. A.A. FOUJDAR, *Implementing Privacy by Design through Privacy Impact Assessments* (tesi di laurea), Turku, 2019, 28-31, in Rete: *https://urn.fi/urn:nbn:fi-fe2019061019771*. Per approfondire il contenuto dei criteri di certificazione v. DELOITTE, *Privacy by Design Certification Program: Assestment Control Framework - Privacy by Design: Privacy Assessment Methodology*, 2016, in Rete: *https://www.torontomu.ca/content/dam/pbdce/certification/Privacy-by-Design-Certification-Program-Assessment-Methodology_PbDCE.pdf*.

[39] Il rinnovo, infatti, richiede un attestato da parte dell'organizzazione che non vi è stata alcuna modifica che influisce sulla loro certificazione. Inoltre, dovrà essere pagata una tariffa di rinnovo della *Privacy By Design Certification Shield*. Cfr. ENISA, *Recommendations on European Data Protection Certification*, *op. cit.*, 42-43; A. CAVOUKIAN, M. CHIBBA, *Privacy Seals in the USA, Europe, Japan, Canada, India and Australia*, *op. cit.*, 77-78.

[40] Cfr. EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, G. BODEA, K. STUURMAN, M. BREWCZYŃSKA, *Data protection certification mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679: annexes*, *op. cit.*, 68-69.

dei dati trattati. Inoltre, come per le certificazioni europee, la Privacy by Design Certification Shield attribuisce un marchio distintivo rispetto alle altre organizzazioni, incrementando la fiducia dei terzi e dei consumatori nei prodotti e processi certificati e ottenendo, così, un notevole vantaggio competitivo. Infine, a livello operativo, la certificazione permetterà di gestire meglio i possibili *data breach* per evitare conseguenze pregiudizievoli agli interessati e garantirne la fiducia nei propri prodotti e servizi[41].

In conclusione, il fervente sviluppo degli strumenti co-regolativi è evidente anche dal fatto che nel *Consumer Privacy Protection Act* si ha intenzione di valorizzare codici di condotta e certificazioni per garantire più facilmente alle imprese di essere conformi alla normativa a protezione dei dati personali. Tali meccanismi, quindi, andrebbero ad assolvere allo scopo di dimostrare la propria *compliance* e il rispetto del principio di *accountability*, ottenendo i medesimi effetti attenuanti garantiti, ad esempio, dal GDPR e scaturendo un notevole vantaggio competitivo alle organizzazioni certificate.

4 USA: Le certificazioni privacy e il *Data Privacy Framework*

Il diritto alla privacy è nato nell'ordinamento statunitense. Come si è accennato nel primo capitolo, la vocazione originaria della privacy era puramente passiva, relativa, infatti, al *right to be let alone*, cioè al diritto di non subire interferenze nella propria vita privata e personale[42]. Quest'ultimo, tuttavia, non era espressamente riconosciuto dall'ordinamento giuridico statunitense ma frutto della progressiva interpretazione estensiva della tutela della personalità avvenuta nel corso del XIX secolo ad opera della dottrina e giurisprudenza statunitense. Da ciò, si è avuta la diffusione del *right to privacy* nel *tort law* dell'ordinamento americano, con l'identificazione di quattro illeciti: *intrusion upon seclusion or solitude, or into the plaintiff's private affairs*; *public disclosure of embarrassing private facts*; *appropriation of name or likeness*; *false light in the public eye*. Ognuno di questi *torts*, tuttavia, si lega alla dimensione della privacy consistente nell'evitare intrusioni nella propria vita privata, senza alcuna considerazione del patrimonio informativo costituito dai dati personali. La riservatezza come *informational privacy* sarà riconosciuta solo a partire dal 1970, anno in cui viene emanato il *Privacy Act*. Questo testo normativo federale, ancora oggi in vigore, si occupa di regolare i rapporti tra governo e individui rispetto alla raccolta, archiviazione e utilizzo delle informazioni (e non dei dati) riferibili ai singoli che siano contente nelle banche dati delle agenzie federali. Tuttavia, come con il *Privacy Act* canadese, la normativa federale statunitense non va a tutelare la protezione delle informazioni personali rispetto ai rapporti tra privati.

Questo determina che al momento non vi è alcuna legge federale comprensiva sulla privacy che protegga le informazioni personali degli individui. Invece, un mosaico

[41] Cfr. B. SOOKMAN, *Privacy by Design certification framework launched by Ryerson and Deloitte*, 2015, in Rete: *https://www.barrysookman.com/2015/05/25/privacy-by-design-certification-framework-launched-by-ryerson-and-deloitte/.*

[42] Cfr. A.C. RAUL, T.D. MANORANJAN, V. MOHAN, *United States*, in A.C. RAUL (a cura di), *The Privacy, Data Protection and Cybersecurity Law Review*, 2014, 268-270, in Rete: *https://www.sidley.com/-/media/files/publications/2014/11/the-privacy-data-protection-and-cybersecurity-la__/files/united-states/fileattachment/united-states.pdf*.

di leggi e regolamenti federali regolano la raccolta e la divulgazione di informazioni personali su base puramente settoriale, venendo differentemente affrontate dal Legislatore americano. Le leggi federali che regolano la protezione delle informazioni personali riguardano, a titolo esemplificativo, i rapporti di credito al consumo, le comunicazioni elettroniche, registri dell'agenzia federale, le informazioni relative all'istruzione, le informazioni bancarie, le informazioni sanitarie, la tutela delle informazioni personali dei minori e la tutela delle informazioni finanziarie[43]. Inoltre, la frammentata regolazione federale dell'*informational privacy* ha portato altresì diversi stati a dotarsi di una propria legislazione generale sulla protezione dei dati personali[44], aggravando ulteriormente il contesto normativo statunitense.

Lo sviluppo di regolamentazione della *data privacy* prettamente settoriale determina importanti conseguenze non solo di natura strettamente legislativa o politica, ma principalmente di natura ordinamentale e di sistema. Infatti, è stato riconosciuto come un approccio normativo generale ed omnicomprensivo (come quello europeo del GDPR) sarebbe incompatibile nell'ordinamento americano, in quanto sarebbe in conflitto con le numerose legislazioni federali settoriali[45].

A fronte di tale criticità, diverse istituzioni hanno tentato di adottare un approccio di *soft-law* al fine di modernizzare l'*information privacy* e di conformarne la tutela similmente a quanto previsto in altri contesti giuridici. Sul punto, di notevole importanza sono stati i menzionati *Fair Information Practice Principles*[46], elaborati dal Department of Health, Education, and Welfare Advisory Committee e successivamente declinati in differenti misure dalle diverse agenzie e dipartimenti statunitensi[47]. Con questi principi si è inteso porre una serie di criteri relativi agli obblighi e alle responsabilità che i diversi operatori hanno quando raccolgono e trattano dati personali, cercato di armonizzare il concetto statunitense di privacy con quello della *data protection* riconosciuto a livello internazionale. Tale risultato, tuttavia, non è stato pienamente raggiunto. La giurisprudenza americana, infatti, pur riconoscendo pienamente a livello costituzionale un diritto alla riservanon è costante nel ritenere sussistente un diritto all'*informational*

---

[43] Cfr. M. BHASIN, *Challenge Of Guarding Online Privacy: Role of Privacy Seals And Government Regulations*, *op. cit.*, 66-67. Per un elenco più esaustivo v. P. GUARDA, G. BINCOLETTO, *Diritto comparato della privacy e della protezione dei dati personali*, *op. cit.*, 32-34.

[44] Al momento solo cinque stati hanno promulgato delle leggi nazionali aventi ad oggetto la protezione della *data privacy* dei consumatori: California, Colorado, Connecticut, Utah and Virginia. Cfr. NCSL, *State Laws Related to Digital Privacy*, 2022, in Rete: *https://www.ncsl.org/technology-and-communication/state-laws-related-to-digital-privacy#:~:text=Five%20states%E2%80%94California%2C%20Colorado%2C,of%20personal%20information%2C%20among%20others.*

[45] Cfr. P. GUARDA, G. BINCOLETTO, *Diritto comparato della privacy e della protezione dei dati personali*, *op. cit.*, 35.

[46] Cfr. *supra*, nota 65.

[47] Per approfondire v. HOMELAND SECURITY DEPARTMENT, *The Fair Information Practice Principles* (aggiornato al 2015), 2008, in Rete: *https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles*; FTC, *Privacy Online: Fair Information Practices in the electronic marketplace*, 2000, in Rete: *https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf*; U.S. GOVERNMENT ACCOUNTABILITY OFFICE, *Comparison of Federal Agency Practices With FTC's Fair Information Principles*, 2000, in Rete: *https://www.gao.gov/assets/gao-01-113t.pdf*.

privacy[48]. A livello legislativo, invece, la *data privacy law* è un assortimento sconcertante di numerose leggi federali e statali che differiscono significativamente l'una dall'altra[49].

In un tale contesto, quindi, le istituzioni pubbliche e private hanno fatto principalmente affidamento all'autoregolamentazione e alla co-regolamentazione sviluppate dalle associazioni del settore. Tuttavia, anche in tale frangente, la protezione dei dati personali non era oggetto di normazione, in quanto si intendeva originariamente regolare la protezione della privacy dei consumatori su internet. A partire dai primi anni del 2000, quindi, cominciarono a svilupparsi le prime iniziative per regolare le pratiche commerciali degli operatori online. In particolare, cominciarono a svilupparsi delle certificazioni che attestassero il rispetto per la riservatezza dei consumatori statunitensi da parte dei siti web che intendessero certificarsi. Alcuni fra questi meccanismi di certificazione avevano, inoltre, una portata internazionale, in quanto i rispettivi criteri sarebbero stati ancorati ai principi internazionali impartiti per la protezione dei dati personale, surclassando, idealmente, la legislazione settoriale sulla *informational privacy*[50].

I meccanismi di certificazione della privacy negli Stati Uniti hanno, quindi, conseguito un'importante importanza in ragione delle potenzialità dello strumento a standardizzare la gestione di quella *informational privacy* che manca tanto nella legislazione statunitense, quanto nella medesima giurisprudenza. Le certificazioni privacy, inoltre, avrebbero dovuto contribuire a sviluppare la fiducia dei consumatori nelle piattaforme web mediane un'attestazione fornita da un'istituzione terza. Quest'ultima, dato che avrebbe il compito di certificare gli operatori online, doveva essere fondata su caratteristiche di terzietà ed imparzialità e, in ragione delle proprie competenze nel settore, avrebbe dovuto potenzialmente trasferire agli enti certificati la fiducia che i terzi e i consumatori avrebbero riposto nell'istituzione certificatrice[51].

In particolare, come identificato da un gruppo di esperti, le certificazioni privacy avrebbero dovuto intervenire su tre punti, in base ai quali possono quindi essere classificate, ossia se contribuiscono a garantire la privacy dei consumatori, se assicurano la sicurezza delle loro informazioni o se salvaguardano l'integrità delle transazioni effettuate online. Ogni certificazione avrebbe dovuto perseguire una o più di queste

[48] Cfr. P. GUARDA, G. BINCOLETTO, *Diritto comparato della privacy e della protezione dei dati personali*, *op. cit.*, 31.

[49] Cfr. D.J. SOLOVE, P.M. SCHWARTZ, *ALI Data Privacy: Overview and Black Letter Text*, in *U.C.L.A. Law Review*, 2022, 1254-1255, in Rete: *https://paulschwartz.net/wp-content/uploads/2022/02/Solove-Schwartz-ALI-Data-Privacy-UCLA-L-Rev-2022.pdf*.

[50] Il vantaggio delle certificazioni privacy, quale mezzo di autoregolamentazione attraverso le associazioni di categoria, sarebbe stato quello di adattarsi più rapidamente e adeguatamente alle innovazioni tecnologiche rispetto alla legislazione statale o federale. Cfr. FTC, *Protecting consumer privacy in an era of rapid change. Recommendations for businesses and policymakers*, 2012, 2-14, in Rete: *https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf*.

[51] Cfr. S. LISTOKIN, *Does Industry Self-Regulation of Consumer Data Privacy Work?*, in *UIC John Marshall Journal of Information Technology & Privacy Law*, Vol. 32, Iss. 1, 2015, 17-19, in Rete: *https://repository.law.uic.edu/jitpl/vol32/iss1/2/*.

'funzioni', a seconda della struttura dei criteri di certificazione, determinando il rafforzamento della fiducia dei consumatori nei servizi online[52].

Attraverso, quindi, la costruzione di un meccanismo fiduciario tra i consumatori, l'ente certificatore e gli organismi certificati, le organizzazioni che non rispetterebbero la *data privacy*, e quindi che non potrebbero accedere ad un mezzo di certificazione, sarebbero state espunte dal mercato, a vantaggio di tutti quegli enti che avrebbero potuto vantare un marchio attestante la propria *compliance privacy*[53].

Altro elemento di importanza è il fatto che i principali meccanismi di certificazione non erano basati sulla legislazione settoriale statunitense, ma poggiavano, invece, sui principi riconosciuti a livello internazionale per la protezione dei dati personali.

Negli Stati Uniti, sono tre le organizzazioni principali il cui scopo è garantire che i siti web mantengano standard di privacy adeguati: Better-Business-Bureau Online (BBBOnLine), AICPA WebTrust, and TRUSTe.

In questo capitolo si tratterà principalmente del meccanismo di certificazione TRUSTe in quanto il più diffuso e, soprattutto, il più controverso nel continente americano[54].

Lo schema di certificazione TRUSTe, sviluppato da TrustArc Inc, è un modello di gestione dei dati personali utilizzabile per le piattaforme online. La certificazione riguarda principalmente la trasparenza e la possibilità di scelta dei consumatori, prevedendo l'obbligo per cui le imprese debbano implementare protezioni commercialmente ragionevoli per la sicurezza dei dati. TRUSTe basa i suoi criteri, in parte, sui FTC *Fair Information Practice Principles*, sui principi NAI (*Network Advertising Initiative*) e sui principi DAA (*Digital Advertising Alliance*). Il sigillo richiede una ricertificazione annuale e il servizio di risoluzione delle controversie dei consumatori elabora migliaia di reclami dei consumatori ogni anno[55]. I criteri di certificazione di TRUSTe e possono essere classificati in diverse categorie concernenti: la limitazione del trattamento; uso di informazioni personali[56]; scelta; raccolta e uso di informazioni personali di terze parti; profili pubblici degli utenti; accesso; comunicazioni promozionali e newsletter; modifiche sostanziali; sicurezza dei dati; qualità e integrità dei dati; *data*

[52] Cfr. K. KYONGSEOK, K. JOOYOUNG, *Third-party Privacy Certification as an Online Advertising Strategy: An Investigation of the Factors Affecting the Relationship between Third-party Certification and Initial Trust*, in *Journal of Interactive Marketing*, 2011, 25(3), 145–158, in Rete: *https://doi.org/10.1016/j.intmar.2010.09.003.*

[53] Proprio sul punto, la certificazione potrebbe fornire una soluzione alle asimmetrie informative che si trovano nel mercato tra le imprese e i consumatori, potendo far distinguere, di primo impatto, i prodotti e i servizi delle imprese rispettosi dei dati personali da quelli che, invece, non ne tengono conto. Cfr. FTC, *Protecting consumer privacy in an era of rapid change. Recommendations for businesses and policymakers*, *op. cit.*, 60-71.

[54] Per approfondire i diversi schemi di certificazione citati v. M. Bhasin, *Challenge Of Guarding Online Privacy: Role Of Privacy Seals And Government Regulations*, *op. cit.*, 63-65.

[55] Cfr. TRUSTARC INC, *TRUSTe Data Collection Certification*, in Rete: *https://trustarc.com/truste-certifications/data-certification/*; EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, G. BODEA, K. STUURMAN, M. BREWCZYŃSKA, *Data protection certification mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679: annexes*, *op. cit.*, 83-88.

[56] Non vengono presi in consdierazione i dati personali, ma le informazioni personali. La differenza consiste nel fatto che per la tutela dell'*informational privacy* è necessario che le informazioni/dati siano direttamente riconducibili ad una persona identificata, mentre non vengono tutelati i dati che permettono un'identificazione solo eventuale del soggetto a cui appartengono.

retention; origini dati di terze parti; *service providers*; formazione; reclami e *feedback* degli utenti; *data breach; accountability* e cooperazione con TrustArc[57].

In ordine al procedimento di certificazione per il marchio TRUSTe, il l'organizzazione titolare della piattaforma online che intende certificarsi deve accettare i principi dello schema e rispettare le procedure di supervisione e monitoraggio del programma di certificazione. I principi di certificazione prevedono che sul sito da asservare deve essere visualizzata una politica sulla privacy che indichi chiaramente quali informazioni personali vengono raccolte ed è, inoltre, richiesto che gli utenti apprestino il proprio consenso al modo in cui tali informazioni vengono utilizzate e condivise. Il sito deve inoltre disporre di adeguate misure di sicurezza per salvaguardare le informazioni degli utenti. Il rispetto di questi principi viene verificato direttamente da TRUSTe, il quale formulerà un rapporto comprensivo in cui sarà dato conto dei risultati relative alla verifica della conformità al programma di certificazione. Al termine con successo di questi passaggi, TRUSTe certifica che il richiedente è conforme ai requisiti del programma[58].

Come detto, la certificazione ha una durata pari ad un anno alla cui scadenza l'organizzazione certificata può rinnovare la certificazione. TRUSTe non attua alcun monitoraggio specifico sulle organizzazioni certificate, tuttavia, nell'eventualità in cui vengano ricevute segnalazioni di terze parti sulle possibili violazioni della certificazione, viene attivato una sorta di procedimento ispettivo mediante il quale la certificazione può essere sospesa o ritirata[59].

Tuttavia, proprio il monitoraggio rappresenta una grave criticità dello schema di certificazione, in quanto nonostante siano previste procedure per la sospensione e la revoca della certificazione, non è chiaro come TRUSTe gestisca in concreto la non conformità. Sono stati, infatti, segnalati casi in cui diverse organizzazioni, pur violando i principi privacy necessari per l'attribuzione del marchio, sono comunque state certificate e risulterebbe, inoltre, che la revoca del sigillo non venga spesso esercitata, mantenendo spesso confidenziali le eventuali violazioni riscontrate. Oltre a ciò, TrustArc, nel 2014, è stata sottoposta ad un procedimento ispettivo della FTC in quanto accusata di non osservare i propri programmi in merito alla ricertificazione annuale per il mantenimento dei marchi di certificazione in oltre 1.000 casi tra il 2006 e il 2013, lasciando che le piattaforme certificate in precedenza mantenessero senza alcun controllo il sigillo[60].

---

[57] Cfr. TRUSTARC, *TRUSTe APEC Privacy Certification Standards*, 2016, in Rete: *https://download.trustarc.com/dload.php/?f=LH7RIJRS-627*.

[58] Cfr. M. BHASIN, *Challenge of Guarding Online Privacy: Role of Privacy Seals and Government Regulations*, *op. cit.*, 63-65; EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, G. BODEA, K. STUURMAN, M. BREWCZYŃSKA, *Data protection certification mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679: annexes*, *op. cit.*, 83-88.

[59] Cfr. EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, G. BODEA, K. STUURMAN, M. BREWCZYŃSKA, *Data protection certification mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679: annexes*, *op. cit.*, 85-86.

[60] Cfr. FTC, *TRUSTe Settles FTC Charges it Deceived Consumers Through Its Privacy Seal Program*, 2014, in Rete: *https://www.ftc.gov/news-events/news/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its-privacy-seal-program*; TRUSTARC INC, *TrustArc's Agreement with the FTC*, 2014, in Rete: *https://trustarc.com/trustarcs-agreement-with-the-ftc/*.

La scarsa capacità di *enforcement* di TrustArc quale ente certificatore nonché la determinante possibilità di abuso della certificazione da parte di terzi evidenzia la natura debole delle certificazioni privacy come TRUSTe negli Stati Uniti. Ciò, in ragione del fatto che gli Organismi di Certificazione non hanno alcun potere reale per affrontare i possibili abusi dei propri schemi. In tali circostanze, la certificazione finirebbe per determinare un cattivo impatto sulla riservatezza e sulla sicurezza delle informazioni. È stato, infatti, dimostrato come i siti web certificati con il marchio TRUSTe abbiano maggiori probabilità di essere classificati come non affidabili rispetto alle piattaforme web non certificati. La certificazione, quindi, aumenterebbe la probabilità di subire *data breach* compromettendo indelebilmente le informazioni personali dei consumatori[61].

Una causa della scarsa efficienza delle certificazioni privacy potrebbe essere proprio quella dell'assenza di norme generali sulla protezione dei dati personali, o comunque di agganci legislativi che permettano anche alle autorità ed agenzie federali di intervenire per sorvegliare la corretta attuazione degli schemi di certificazione. Alcuni gruppi industriali si opposti alla possibilità di introdurre una regolamentazione federale sull'*informational privacy*, ritenendo che la sola autoregolamentazione in questa materia fosse sufficiente e adeguata. Tuttavia, tale posizione non può essere ragionevolmente sostenuta fino a quando non si abbia la certezza che le organizzazioni che gestiscono le certificazioni privacy, come TrustArc, siano in grado di monitorare adeguatamente l'industria digitale e di esercitare poteri di *enforcement* capaci di correggere l'eventuale illecita raccolta o diffusione di dati e informazioni personali[62].

In assenza di tali caratteristiche, l'approccio dell'autoregolamentazione non può funzionare, rischiando di generare possibili abusi da parte delle grandi industrie digitali in danni ai diritti e alle libertà dei consumatori le cui informazioni vengono trattate. In ragione di ciò, sarebbe necessario l'intervento pubblico da parte del Legislatore o del governo statunitense, affinché si possa effettivamente migliorare la privacy degli utenti della rete, facilitando la fiducia nei servizi digitali e attribuendo specifiche responsabilità alle organizzazioni che trattino illecitamente dati e informazioni personali. Due potrebbero essere le soluzioni da seguire: o un intervento legislativo completo e comprensivo sulla materia della protezione dei dati personali, il quale, però, rappresenta una difficile risoluzione da conseguire [63], ovvero adottare un approccio di co-regolamentazione. Quest'ultimo potrebbe essere il modello più facilmente implementabile nell'ordinamento statunitense, il quale potrebbe operare mediante una delle seguenti opzioni:

[61] Cfr. S. LISTOKIN, *Does Industry Self-Regulation of Consumer Data Privacy Work?*, *op. cit.*, 17-19.

[62] Cfr. C.P. O'KANE, *Digital privacy and new media: An empirical study assessing the impact of Privacy Seals on personal information disclosure*, Bournemouth, 2019, 77-78, in Rete: *https://eprints.bournemouth.ac.uk/34340/1/O%E2%80%99KANE%2C%20Conor%20Paul_Ph.D._2019.pdf*.

[63] Proprio a fronte di ciò si segnala il naufragato tentativo del 2022 per l'approvazione dell'*American Data Privacy and Protection Act,* il quale era destinato a diventare la prima legge federale sulla privacy online. Questa proposta di legge federale, pur costituendo un primo tentativo di regolare compiutamente la privacy, non ha riscontrato positivi giudizi ed è stata molto criticata dalle associazioni di categoria nonché dai rappresentanti dello Stato della California, i quali godono già di una propria legge nazionale sulla protezione dei dati.

- la prima, potrebbe consistere nella cooperazione tra le autorità pubbliche e le imprese per procedere alla definizione normativa in modo congiunto delle questioni relative alla protezione dei dati personali;
- la seconda, mediante la delega di poteri regolativi ad un organismo di diritto privato, guidato dalle imprese o comunque dalle associazioni di categoria, che si occupi di normare il settore della protezione dei dati personali, con la vigilanza di un'agenzia federale;
- con la terza opzione, invece, le autorità pubbliche dovrebbero incoraggiare la creazione, e ne valutando e approvandone il contenuto, di schemi e/o meccanismi di autoregolamentazione da parte dell'industria, monitorandone la corretta attuazione sulla base di un'eventuale regolamentazione generica sulla protezione dei dati personali o su principi come i *Fair Information Practices Principles*[64].

In conclusione, proprio sul tema delle certificazioni relative alla protezione dei dati personali nell'ordinamento statunitense non si può non fare riferimento al nuovo accordo politico raggiunto tra gli Stati Uniti e l'Unione europea volto ad apporre delle modifiche alla legislazione statunitense al fine di renderlo compatibile con i requisiti previsti dal GDPR per il trasferimento transfrontaliero di dati personali. Il raggiungimento del *Data Privacy Framework* ha costituito la base per l'adozione da parte della Commissione europea della decisione di adeguatezza del 10 luglio 2023 per permettere il trasferimento di dati personali negli Stati Uniti senza le ulteriori garanzie necessarie richieste dall'art. 46 GDPR[65].

Fermo restando che questo contributo ha lo scopo di fornire una panoramica sullo strumento certificativo come mezzo per attestare la tutela della privacy e della protezione dei dati personali negli Stati Uniti, e non di constatare se effettivamente l'ordinamento statunitense possa essere considerato sostanzialmente equivalente a quello europeo in termini di tutele e garanzie per la protezione dei dati personali[66], è necessario sottolineare che il nuovo UE-US *Data Privacy Framework* si basa proprio sulle certificazioni per attestare la capacità delle imprese statunitensi di rispettare i principi e le garanzie europee previste dal GDPR. I titolari e responsabili del trattamento potranno autocertificare la loro adesione a una serie di principi al fine di poter ricevere e trattare i dati provenienti dall'UE. Il meccanismo sarà amministrato dal Dipartimento del Commercio degli Stati Uniti, che elaborerà le domande di certificazione e monitorerà se le aziende partecipanti continuano a soddisfare i requisiti di certificazione. Quindi, verso tutte le organizzazioni degli Stati Uniti autocertificate ed incluse nella *Data Privacy*

[64] Cfr. R. RODRIGUES, D. WRIGHT, K. WADHWA, *Developing a privacy seal scheme (that works)*, in *International Data Privacy Law*, Vol. 3, Iss. 2, 2013, 112, in Rete: *https://doi.org/10.1093/idpl/ips037*.

[65] Cfr. COMMISSIONE EUROPEA, *Comunicato stampa: Protezione dei dati: la Commissione europea adotta una nuova decisione di adeguatezza per la circolazione sicura e affidabile dei flussi di dati UE-USA*, 2023, in Rete: *https://ec.europa.eu/commission/presscorner/detail/it/ip_23_3721*; COMMISSIONE EUROPEA, *Commission Implementing Regulation (EU) 2023/4745*, 2023, in Rete: *https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_it*.

[66] Per un primo commento alla nuova decisione di adeguatezza v. M. GIACALONE, *Verso Schrems III? Analisi del nuovo EU-US Data Privacy Framework*, in *European Papers*, Vol. 8, 2023, N. 1, 149-157, in Rete: *https://doi.org/10.15166/2499-8249/644*.

Framework List[67] potranno essere trasferiti i dati personali europei sulla base della decisione di adeguatezza, mentre per le organizzazioni non inserite nella lista continueranno ad essere valide le clausole contrattuali standard o le *Binding Corporate Rules* adottate ai sensi dell'art. 46 GDPR.

Lo UE-US *Data Privacy Framework* si basa su una serie di principi mutuati dalla disciplina europea sulla protezione dei dati personali. In particolare, le organizzazioni statunitensi che intendono aderire al Framework devono:

- Informare gli interessati in merito alla tipologia di dati personali raccolti, all'impegno a rispettare i principi del DPF, all'eventualità che i dati personali possano essere trasferiti a terzi con la contestuale indicazione dell'identità di questi ultimi e le finalità di tale trasferimento successivo, al diritto di accesso ai propri dati trattati, all'esistenza di un organismo indipendente per la risoluzione delle controversie relative ai reclami formulati dagli interessati e alla possibilità di accedere alla *Data Protection Review Court*, al fatto che l'organizzazione statunitense sia soggetta alla FTC o al Dipartimento del Commercio degli USA e, infine, alla possibilità che i dati personali trattati possano essere svelati in risposta a richieste legittime da parte delle autorità pubbliche, anche per soddisfare requisiti di sicurezza nazionale o di applicazione della legge[68];
- Assicurare agli interessati il diritto di opporsi affinché i propri dati personali siano divulgati presso terzi oppure che siano utilizzati per uno scopo sostanzialmente differente rispetto a quello per cui sono stati originariamente trattati[69];
- In caso di trasferimento successivo dei dati presso soggetti terzi al DPF, stipulare un contratto o un altro strumento vincolante con il terzo il quale preveda che i dati possano essere trattati solo per finalità limitate e specifiche, sulla base di una legittima base giuridica e sul presupposto che il terzo fornisca lo stesso livello di protezione del DPF. Nel caso in cui il soggetto terzo non possa assicurare il medesimo livello di tutela, il contratto dovrà prevedere l'immediata cessazione del trasferimento e di ogni trattamento, oppure l'adozione di adeguate misure per porvi rimedio[70];
- Adottare misure idonee per proteggere i dati raccolti da ogni possibile violazione, perdita, uso improprio, accesso illecito, divulgazione, alterazione o distruzione non autorizzata, tenendo conto dei rischi connessi in relazione alla natura del trattamento e alla tipologia dei dati trattati[71];
- Trattare i dati compatibilmente con le finalità individuate, in attuazione del principio di limitazione delle finalità. Inoltre, dovranno essere adottate misure

[67] Cfr. U.S. DEPARTMENT OF COMMERCE, *Data Privacy Framework List*, in Rete: *https://www.dataprivacyframework.gov/s/participant-search*.

[68] Cfr. *id*, *Data Privacy Framework Principles: 1. Notice*, in Rete: *https://www.dataprivacyframework.gov/s/article/1-notice-dpf?tabset-35584=2*.

[69] Cfr. *id*, *2. Choice*, in Rete: *https://www.dataprivacyframework.gov/s/article/2-choice-dpf?tabset-35584=2*.

[70] Cfr. *id*, *3. Accountability for onward transfer*, in Rete: *https://www.dataprivacyframework.gov/s/article/3-accountability-for-onward-transfer-dpf?tabset-35584=2*.

[71] Cfr. *id*, *4. Security*, in Rete: *https://www.dataprivacyframework.gov/s/article/4-security-dpf?tabset-35584=2*.

ragionevoli affinché si garantisca che i dati personali siano affidabili, accurati, completi e aggiornati in relazione all'uso previsto[72];

- Assicurare agli interessati il diritto di accesso ai dati personali che li riguardano, permettendone l'eventuale correzione, modifica o cancellazione qualora siano inesatti o i dati siano raccolti in violazione del DPF[73];
- Adottare meccanismi per garantire il rispetto dei principi DPF, un meccanismo di ricorso indipendente per gli interessati i cui dati sono trattati in violazione dei principi, delle procedure di *follow-up* per verificare l'effettiva implementazione dei principi nelle proprie pratiche, nonché per assicurare la piena collaborazione alle indagini o richieste del Dipartimento del Commercio, della FTC o delle Autorità europee per la protezione dei dati[74].

Come detto, possono legittimamente trattare dati europei sulla base della decisione di adeguatezza della Commissione europea le organizzazioni statunitensi che si siano sottoposte al procedimento di autocertificazione previsto dal DPF. La certificazione da questo punto di vista è assolutamente volontaria e non è necessaria per i trattamenti di dati personali che vengono compiuti sulla base degli ulteriori mezzi di garanzia previsti dall'art. 46 GDPR. L'autocertificazione ha una durata annuale e successivamente dovrà essere trasmesso al Dipartimento del Commercio statunitense la propria volontà di aderire al *Framework*.

Una determinata organizzazione, per autocertificarsi sulle parti pertinenti al programma DPF, dovrà fornire al Dipartimento del Commercio una richiesta online, usufruendo della sezione apposita presente nel sito web del DPF. In particolare, sia per la prima volta, che per i rinnovi successivi, l'organizzazione dovrà evidenziare nel modulo le misure attuate per conformarsi ai principi del DPF. Una volta concluso il procedimento di adesione, è bene specificare che le autorità statunitensi non eseguiranno alcun controllo attivo sull'impresa che ha provveduto all'autocertificazione [75]; il Dipartimento del Commercio, si limiterà ad inserire l'organizzazione richiedente nella lista del DPF e ad intervenire, rimuovendola dalla medesima lista, ove a seguito di un procedimento ispettivo si scopra che quest'ultima abbia violato i principi del DPF[76].

La disciplina prevista dal *Data Privacy Framework* evidenzia, quindi, come il processo di armonizzazione internazionale della disciplina sulla protezione dei dati personali avviato dall'UE con il GDPR abbia influenzato anche l'ordinamento americano,

---

[72] Cfr. *id, 5. Data integrity and purpose limitation*, in Rete: *https://www.dataprivacyframework.gov/s/article/5-data-integrity-and-purpose-limitation-dpf?tabset-35584=2*.

[73] Cfr. *id, 6. Access*, in Rete: *https://www.dataprivacyframework.gov/s/article/6-access-dbf?tabset-35584=2*.

[74] Cfr. *id, 7. Recourse, enforcement and liability*, in Rete: *https://www.dataprivacyframework.gov/s/article/7-recourse-enforcement-and-liability-dpf?tabset-35584=2*.

[75] Questo elemento rappresenta una notevole criticità che accomuna il DPF ai precedenti *Privacy Shield* e *Safe Harbor*.

[76] Cfr. U.S. DEPARTMENT OF COMMERCE, *How to Join the Data Privacy Framework (DPF) Program (part 1)*, in Rete: *https://www.dataprivacyframework.gov/s/article/how-to-join-the-data-privacy-framework-dpf-program-part-1-dpf?tabset-35584=1*; *Id*, *(part 2)*, in Rete: *https://www.dataprivacyframework.gov/s/article/how-to-join-the-data-privacy-framework-dpf-program-part-2-dpf*.

tendenzialmente a tradizione liberista, ad inserire un minimo controllo pubblico sulle attività di certificazione per la protezione dei dati personali. A questo punto non si può che sperare che l'influenza determinata dal DPF possa ulteriormente accrescere il grado di interesse delle organizzazioni americane nella protezione dei dati personali determinando lo sviluppo di nuovi meccanismi di certificazione che siano, almeno, in linea con il *Data Privacy Framework*.

CONCLUSIONI

I servizi sia pubblici che privati si basano necessariamente su ampie basi di dati personali. La loro protezione è, quindi, una questione cruciale per lo sviluppo di una società tecnologicamente avanzata. Maggiore è il numero dei dati raccolti, maggiori sono le possibilità di innovazione e di ritorno economico dal loro sfruttamento. Al fine di progredire la ricerca scientifica e accrescere l'influenza verso le multinazionali di settore, i legislatori e i governi di diverse nazioni si stanno impegnando sempre più a raccogliere dati per includerli in appositi *cluster*[1].

La normativa *data protection* costituisce, dunque, un mezzo fondamentale per evitare distorsioni dal corretto utilizzo dei dati rispetto ai diritti, libertà e alla dignità dei singoli individui a cui appartengono.

Il GDPR, come esposto, non dev'essere considerato come un ostacolo alla libera circolazione dei dati, ma come un necessario bilanciamento tra la protezione dei diritti fondamentali dell'individuo e la libera circolazione ed uso dei suoi dati. Indubbiamente, il Regolamento introduce alcuni elementi che non sono completamente chiari e difficili da determinare, come il principio di *accountability*. Quest'ultimo, impone che il titolare o il responsabile del trattamento analizzino e comprendano i possibili rischi per gli interessati, catalogandone la portata e il possibile impatto, e adottino ogni misura tecnica od organizzativa più idonea per mitigarne la gravità dell'impatto o la probabilità dell'avverarsi di una minaccia.

Tale inciso, tuttavia, pur riproducendo la definizione del principio di *accountability*, non permette di chiarificarne totalmente la portata impedendone la sua intellegibile applicazione. Di conseguenza, ad esclusione dei casi di conclamato trattamento illecito dei dati personali, non sempre l'inosservanza del GDPR di un'organizzazione è determinata da colpa del titolare o del responsabile del trattamento. Il vero problema, infatti, diviene principalmente quello dell'interpretazione soggettiva che può essere formulata per l'applicazione del principio di cui all'art. 6, par. 2 e agli altri adempimenti connessi. L'effettività del diritto alla protezione dei dati personali, quindi, rischierebbe, potenzialmente, di essere compromessa in assenza di interpretazioni autorevoli che stabiliscano quali siano le misure da implementare e come svilupparle.

Le varie Linee Guida dell'EDPB e i provvedimenti delle diverse autorità nazionali di protezione dei dati personali possono aiutare nell'uniformare l'interpretazione e l'applicazione delle norme ed obblighi del Regolamento, ma la loro attività potrebbe non essere, se non sufficiente, quantomeno tempestiva.

Per tale ragione la prassi ha progressivamente cominciato a legarsi, realizzando regole tecniche le quali, più che mettere in discussione l'autorità legislativa, intendono fornire un'interpretazione ragionevolmente oggettiva ed uniforme. Standard tecnici, protocolli di cybersicurezza e *audit* informatici, d'altronde, permettono di vincolare i

[1] Con il termine *cluster* si intende un insieme di elementi che hanno una o più caratteristiche in comune tra loro. Attraverso la *cluster analysis*, la statistica permette di processare i dati, raggruppando gli elementi di un insieme in classi non assegnate a priori.

privati molto più di quanto possano fare delle norme giuridiche eccessivamente astratte. Seguendo questa logica, le regole di prassi tanto più sono rigide, quanto più ne è facile l'applicazione, garantendo risparmi di costi, tempo e risorse umane. Tutto ciò, assicurando costantemente un'adeguata protezione ai diritti e alle libertà degli interessati.

Il GDPR ha recepito due tra i principali meccanismi di autoregolamentazione privata, ossia certificazioni e codici di condotta. Il fatto che questi ultimi siano ancorati a delle norme giuridiche, muta la natura di questi strumenti da autoregolativi a mezzi di co-regolamentazione, garantendone una più efficacie e controllata applicazione. Con questa iniziativa sicuramente la 'libertà' e l'autonomia dei privati nella formalizzazione autonoma di regole è in parte diminuita; tuttavia, come si è cercato di dimostrare nei precedenti capitoli, un controllo pubblico, che sia parziale o integrale, è necessario nella regolamentazione privata della *data protection* al fine di scongiurare possibili abusi.

Gli strumenti di co-regolamentazione e, in particolare, i meccanismi di certificazione possono essere quindi considerati un valido strumento nell'indirizzare i titolari e responsabili del trattamento nell'adottare le misure più idonee per la protezione dei dati personali?

La presente tesi di laurea ha avuto proprio come scopo quello di raccogliere gli elementi principali per poter rispondere a questa domanda. Secondo chi scrive, infatti, le certificazioni rappresentano un'importante opportunità per gestire la *compliance* relativa alla protezione dei dati personali assolutamente efficacie, anche se non ancora pienamente esplorata. Ad oggi, infatti, se il tema non è di frequente trattazione in dottrina, nel mondo imprenditoriale è pressoché sconosciuto. Tuttavia, come si è visto, è il medesimo Regolamento a riconoscere particolare rilevanza alle certificazioni, come mezzo adeguato a soddisfare gli adempimenti previsti dallo stesso. Le certificazioni, infatti, vengono richiamate nelle principali norme relative al principio di *accountability*: l'art. 25, par. 3 (Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita); l'art. 32, par. 3 (Sicurezza del trattamento); l'art. 46, par. 2, lett. e) (Trasferimento soggetto a garanzie adeguate); l'art. 28, par. 5-6 (Responsabile del trattamento); l'art. 24, par. 3 (Responsabilità del titolare del trattamento), rispetto al quale si agganciano comunque tutti gli obblighi previsti dal GDPR per il titolare del trattamento.

Le certificazioni sono quindi un'opportunità per chi è attivamente coinvolto nel trattamento dei dati personali, a condizione che vengano garantiti elevati standard di qualità e trasparenza.

A seguito dell'analisi delle norme che regolano le certificazioni per la protezione dei dati personali, una critica può essere formulata rispetto alla loro chiarezza. Gli artt. 42 e 43 GDPR appaiono complessi e intricati rispetto all'approvazione dei criteri di certificazione e all'iter per l'assegnazione della certificazione alle organizzazioni che ne fanno richiesta.

Nel primo caso, infatti, mancano totalmente nel Regolamento delle indicazioni che rappresentino come creare i criteri di certificazione e quali obblighi della protezione dei dati personali siano da seguire. Sul punto è comunque intervenuto l'EDPB, con le Linee Guida 1/2018, e successivamente le altre autorità di controllo nazionali, evidenziando come debbano essere considerati alla base dello sviluppo dei criteri tutti gli obblighi del

Regolamento. Tuttavia, sarebbe stato auspicabile, o quanto meno opportuno, illustrare già nell'art. 42 GDPR questo aspetto, tenendo anche in conto che non sempre gli schemi di certificazione possono avere ad oggetto genericamente un intero trattamento, ma anche una sola sezione dello stesso.

Lo stesso vale per il secondo caso, in quanto gli artt. 42 e 43 non contengono alcuna informazione né sulla procedura di certificazione delle organizzazioni che ne fanno richiesta, né sulla metodologia di *audit* che gli OdC devono adottare. Entrambi i punti sono rimessi alla discrezionalità degli *scheme owner* e degli OdC, mentre le norme in questione prevedono solamente che la certificazione sia attribuita sulla base di una procedura trasparente e che agli OdC venga fornita ogni informazione ed accesso ai trattamenti da verificare e alla relativa documentazione. La soluzione certificativa presuppone precisione e chiarezza, tanto rispetto alla definizione dello schema, quanto in relazione alle procedure per l'attribuzione dello stesso. Ebbene, poteva essere opportuno inserire nel GDPR dei principi che guidassero gli operatori nello sviluppo di un procedimento di certificazione armonizzato e non eccessivamente eterogeneo tra i diversi meccanismi di certificazione. In ogni caso, al momento, il rischio di potenziali disfunzioni nella procedura di certificazione è sventato dalla verifica preliminare delle autorità di controllo nazionali in sede di approvazione dei criteri di certificazione.

Infine, si può esprimere un'identica critica in relazione alla metodologia di *audit* che i OdC devono adottare per verificare la conformità dell'ente che intende certificarsi. Il Regolamento nulla dice al riguardo e anche in questo caso vengono in aiuto gli standard tecnici ISO. Infatti, la norma UNI EN ISO 19011:2018 definisce, in generale, l'*audit* come un "*processo sistematico, indipendente e documentato utilizzato al fine di ottenere evidenze oggettive e valutarle con obiettività, al fine di determinare in quale misura i criteri dell'audit sono soddisfatti*". Orbene la necessità di raccogliere evidenze oggettive e valutarle obiettivamente è assolutamente essenziale per costruire una procedura di certificazione sana che possa garantire la trasparenza; tuttavia, non si comprende come questi elementi non siano stati sottolineati anche dal GDPR. L'art. 43 attribuisce sicuramente assoluta importanza alla competenza delle risorse appartenenti all'Organismo di Certificazione al fine del loro necessario accreditamento e tale requisito potrebbe in parte collegarsi ad un possibile controllo delle modalità di *auditing* previste dall'OdC da parte dell'autorità preposta a rilasciare l'accreditamento. Ciononostante, questa ricostruzione non è appieno convincente proprio in ragione del dato letterale. L'art. 43, par. 2, lett. c) prevede, infatti, che l'ente preposto all'accreditamento verifichi solamente se gli OdC abbiano "*istituito procedure per il rilascio, il riesame periodico e la revoca delle certificazioni, dei sigilli e dei marchi di protezione dei dati*", senza entrare nel merito di constatare specificamente l'efficacia delle procedure di verifica adottate per il rilascio. Probabilmente, anche in tale occasione, fornire dei principi ovvero dei criteri che evidenziassero i campionamenti essenziali da svolgere per la certificazione o, quantomeno, che guidassero nell'adozione di un metodo di verifica basato su delle linee essenziali comuni tra i vari OdC, sarebbe stato più opportuno.

Ciò non toglie che, rispetto a tutte le criticità individuate, la Commissione europea possa adottare un atto delegato, conformemente all'art. 92 GDPR, al fine di precisare i requisiti di cui tenere conto per i meccanismi di certificazione della protezione dei dati,

ovvero di adottare atti di esecuzione per stabilire norme tecniche riguardanti i meccanismi di certificazione, ai sensi dell'art. 43, par. 8-9 del Regolamento.

L'auspicio finale è che con questo elaborato si sia fornita una più chiara panoramica delle certificazioni ai sensi del GDPR. Queste ultime sicuramente non potranno essere una soluzione esaustiva a tutte le criticità che caratterizzano il trattamento di dati personali, specialmente negli scenari più complessi; esse possono, però, offrire delle valide fondamenta per progettare efficacemente le misure tecniche ed organizzative necessarie per soddisfare il principio di *accountability*. L'adesione ad un meccanismo di certificazione, così come ad un codice di condotta, rappresenta la migliore opzione per garantire la trasparenza e la sicurezza di un trattamento di dati personali, incrementando potenzialmente la fiducia degli interessati nei servizi digitali e nelle nuove tecnologie.

BIBLIOGRAFIA

Alpa G., *Autodisciplina e codici di condotta*, in *Sociologia del diritto*, fasc. 2, 1995, 128 ss.

Amore G., *Fairness, Transparency e Accountability nella protezione dei dati personali*, in *Studium Iuris*, 2020, n. 4, 414-429.

Annecca T., *Codici deontologici e il GDPR*, in R. Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Milano, 2019, 621-640.

Arcella G., *GDPR: il Registro delle attività di trattamento e le misure di accountability,* in *Notariato*, 2018, n. 4, 393-398.

Baldassarre A., *Globalizzazione contro democrazia*, Roma-Bari, 2002.

Basunti C., *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in *Contratto e impresa*, 2020, vol. 26, n. 2, 860-895.

Bellisario E., *Certificazioni di qualità e responsabilità civile*, Milano, 2011.

Bennett R., Kottasz R., *Practitioner perceptions of corporate reputation: an empirical investigation*, in *Corporate Communications: An International Journal*, 2000, vol. 5, n.4, 224-234.

Bhasin M., *Challenge Of Guarding Online Privacy: Role Of Privacy Seals And Government Regulations*, in *South Asian Journal of Marketing & Management Research*, 3 (2), 2016, 59-75, in Rete: *https://www.researchgate.net/publication/309407924_challenge_of_guarding_online_privacy_role_of_privacy_seals_and_government_regulations*.

Bilgesu S., *The Certification Mechanism Under the EU General Data Protection Regulation* (tesi di laurea), Istanbul, 2019, in Rete: *https://www.proquest.com/dissertations-theses/certification-mechanism-under-eu-general-data/docview/2495414321/se-2*.

Bincoletto G., *La privacy by design: un'analisi comparata nell'era digitale*, Roma, 2019.

Bistolfi C., *Adozione obbligatoria di strumenti per la sicurezza del trattamento: adozione di specifici strumenti*, in C. Bistolfi, L. Bolognini, E. Pelino*, Il Regolamento Privacy Europeo,* Milano, 2016, 400-409.

Bistolfi C., *Principi da osservare*, in C. Bistolfi, L. Bolognini, E. Pelino (a cura di), *Il Regolamento Privacy Europeo*, Milano, 2016, 323- 343.

Bolognini L., *Art. 20 – Codici di deontologia e di buona condotta vigenti alla data di entrata in vigore del presente decreto*, in Bolognini, E. Pelino, I. M. Alagna (a cura di), *Codice della disciplina privacy*, Milano, 2019, 285-291.

Bolognini L., *Art. 2-septiesdecies – Organismo nazionale di accreditamento*, in L. Bolognini, E. Pelino, I. M. Alagna (a cura di), *Codice della Disciplina Privacy*, Milano, 2019, 300-302.

Bolognini L., *Art. 40 – Codici di condotta*, in Bolognini, E. Pelino, I. M. Alagna (a cura di), *Codice della disciplina privacy*, Milano, 2019, 283.

Bolognini L., *Art. 42 – Certificazione*, in L. Bolognini, E. Pelino, I. M. Alagna (a cura di), *Codice della Disciplina Privacy*, Milano, 2019, 294-297.

Bolognini L., *Art. 43 – Organismi di certificazione*, in L. Bolognini, E. Pelino, I. M. Alagna (a cura di), *Codice della Disciplina Privacy*, Milano, 2019, 297-300.

Bolognini L., *Codici di condotta*, in L. Bolognini, C. Bistolfi, E. Pelino (a cura di), *Il Regolamento Privacy europeo*, Milano, 2019, 421-437.

Bolognini L., *Obbligo di documentazione*, in C. Bistolfi, L. Bolognini, E. Pelino (a cura di), *Il Regolamento Privacy Europeo*, Milano, 2016, 413-420.

Bolognini L., Ziegler S., intervento presentato al seminario *Il meccanismo delle certificazioni con il GDPR – Il primo sigillo europeo per la protezione dei dati: la certificazione di Europrivacy*, 22 novembre 2022, in Rete: *https://www.federprivacy.org/attivita/webinar-sul-meccanismo-delle-certificazioni-con-il-gdpr-e-il-primo-sigillo-europeo-sulla-protezione-dei-dati.*

Bravo F., *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I Dati Personali Nel Diritto Europeo*, Torino, 2019, 775- 853.

Calzolaio S., *Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679,* in *federalismi.it*, 2017, n. 24, in Rete: *https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=35361*.

Caringella F., *La tutela aquiliana della privacy nel Codice per la protezione dei dati personali (d.lgs. n. 196/2003)*, in *Studi di Diritto civile, III. Obbligazioni e responsabilità,* 2007.

Casonato C., Marchetti B., *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw Journal – Rivista di BioDiritto*, n. 3/2021, 415-437, in Rete: *https://iris.unitn.it/retrieve/handle/11572/318571/516882/document(1).pdf*.

Castroreale R., Ponti C., *Il sistema integrato per la sicurezza delle informazioni ed il GDPR: guida operativa all'efficace integrazione dei due mondi anche con l'ausilio della ISO/IEC 27701*, Roma, 2021.

Cavoukian A., Chibba M., *Privacy Seals in the USA, Europe, Japan, Canada, India and Australia*, in R. Rodrigues, V. Papakonstantinou (a cura di) *Privacy and Data Protection Seals*, 59-82.

Cavoukian A., *Privacy by design, The 7 Foundational Principles*, Canada, 2011.

Cavoukian A., Taylor S., Abrams M.E., *Privacy by Design: essential for organizational accountability and strong business practices*, IDIS 3, 2010, 405–413.

Colapietro C., *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello. Il regolamento UE 2016/679 parametro di legittimità della complessiva normativa sulla privacy*, Napoli, 2018.

Colarocco V., Previti S. (a cura di), *GDPR e digitalizzazione dei processi aziendali*, Milano, 2019.

Coraggio G. (a cura di), *Privacy e Data protection 2022, IPSOAInPratica,* 2022.

D'acquisto G., Naldi M., Pizzetti F., *Big data e privacy by design: anonimizzazione pseudonimizzazione sicurezza*, Torino, 2017.

D'orazio R., *Articolo 40 – Codici di condotta*, in E. Belisario, G.M. Riccio, G. Scozza (a cura di), *GDPR e Normativa Privacy*, Milano, 2020, 445-467.

E. Lachaud, *What GDPR tells about certification*, in *Computer Law & Security Review*, V. 38, 2020, in Rete: *https://doi.org/10.1016/j.clsr.2020.105457*.

Emegian F., Perego M., Bernardi N., *Privacy & audit: aggiornato al Regolamento europeo UE 216/679*, Milano, 2017.

European Commission, Directorate-General for Justice and Consumers, Bodea G., Stuurman K., Brewczyńska M., *Data protection certification mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679: final report*, 2019, in Rete: *https://data.europa.eu/doi/10.2838/115106.*

European Commission, Directorate-General for Justice and Consumers, Bodea G., Stuurman K., Brewczyńska M., *Data protection certification mechanisms – Study on Articles 42 and 43 of the Regulation (EU) 2016/679: annexes*, 2019, in Rete: *https://data.europa.eu/doi/10.2838/297807*.

Faccioli E., Cassaro M., *Il "GDPR" e la normativa di armonizzazione nazionale alla luce dei principi: accountability e privacy by design*, in *Il Diritto industriale*, 2018, n. 6, 561-566.

Faillace S., *La natura e la disciplina delle obbligazioni id cui all'art. 25 GDPR*, in *Contratto e Impresa*, 2022, n. 4, 1223-1148

Fancello V., *Certificazione dei corrispettivi elettronici: processi, tecnologie e punti di controllo IT*, in *Amministrazione & Finanza*, 2019, n. 12, 62-63.

Finocchiaro G., *Il principio di accountability*, in *Giurisprudenza italiana*, 2019, vol. 171, fasc. 12, 2778-2783.

Finocchiaro G., *Introduzione al regolamento europeo sulla protezione dei dati*, in *Le Nuove Leggi Civili Commentate*, 2017, vol. 40, fasc. 2, 1-18.

Foujdar A.A., *Implementing Privacy by Design through Privacy Impact Assessments* (tesi di laurea), Turku, 2019, in Rete: *https://urn.fi/urn:nbn:fi-fe2019061019771*.

Franceschelli V., *Premesse,* in E. Tosi (a cura di), *Privacy digitale: riservatezza e protezione dei dati personali tra* GDPR *e nuovo Codice Privacy,* Milano, 2019, XXXVII *ss*.

Gambini M., *Responsabilità e risarcimento nel trattamento dei dati personali*, in V. Cuffaro, R. D'Orazio, V. Ricciuto, *I Dati Personali Nel Diritto Europeo*, Torino, 2019, 1017-1092.

Gawer A., *Digital platforms and ecosystems: remarks on the dominant organizational forms of the digital age*, in *Innovation: Organization & Management*, 2022, Vol. 24, N. 1, 110-124, in Rete: *https://doi.org/10.1080/14479338.2021.1965888*.

Gellert R., *Understanding the notion of risk in the General Data Protection Regulation,* in *Computer Law & Security Review*, 2018, vol. 34, issue 2, 279-288.

Giannetti R., *La certificazione ai sensi del GDPR: standard per l'affidabilità del mercato data-driven*, in L. Bolognini (a cura di), *Privacy e libero mercato digitale: convergenza tra regolazioni e tutele individuali nell'economia data-driven*, Milano, 2021, 217-237.

Giardina C.C., *Il Data breach in ambito sanitario: l'importanza di una corretta policy per evitare san-zioni da parte del Garante della Privacy*, in *Azienditalia*, 2021, n. 6, 1067-1062.

Grafenstein M., *Co-Regulation and the Competitive Advantage in the GDPR: Data protection certification mechanisms, codes of conduct and the "state of the art" of data protection-by-design*, in G. González-Fuster, R. Brakel, P. De Hert (a cura di), *Research*

Handbook on Privacy and Data Protection Law, 2019, in Rete: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3336990*.

Guarda P., Bincoletto G., *Diritto comparato della privacy e della protezione dei dati personali*, Zenodo, 2023, in Rete: *https://doi.org/10.5281/zenodo.7805085*.

Guastalla E.L., *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contratto e impresa*, 2018, n. 1, 106-125.

Hacker P., *A Legal Framework for AI Training Data - From First Principles to the Artificial Intelligence Act*, in *Law, Innovation and Technology*, 2021, in Rete: *https://ssrn.com/abstract=3556598*.

Helmke J.T., Link H., Schild H.H., *Zertifizierungskriterien für Verarbeitungstätigkeiten*. In *Datenschutz Datensich*, Vol. 47, 2023, 100–107, in Rete: *https://doi.org/10.1007/s11623-023-1725-9*.

Imperiali R., *Codice della privacy. Commento alla normativa sulla protezione dei dati personali*, Milano, 2005.

Kyongseok K., Jooyoung K., *Third-party Privacy Certification as an Online Advertising Strategy: An Investigation of the Factors Affecting the Relationship between Third-party Certification and Initial Trust*, in *Journal of Interactive Marketing*, 2011, 25(3), 145–158, in Rete: *https://doi.org/10.1016/j.intmar.2010.09.003.*

Lipari N., *La formazione negoziale del diritto*, in *Riv. dir. civ.*, 1987, I, 307–316.

Listokin S., *Does Industry Self-Regulation of Consumer Data Privacy Work?*, in *UIC John Marshall Journal of Information Technology & Privacy Law*, Vol. 32, Iss. 1, 2015, 17-19, in Rete: *https://repository.law.uic.edu/jitpl/vol32/iss1/2/*.

Mantelero A., *Responsabilità e rischio nel Reg. UE 2016/679*, in *Le Nuove Leggi Civili Commentate,* 2017, n. 1, 144-164.

Marsch N., *Artificial Intelligence and the Fundamental Right to Data Protection: Opening the Door for Technological Innovation and Innovative Protection*, in T. Wischmeyer, T. Rademacher (a cura di), *Regulating Artificial Intelligence*, 34-50, 2020, in Rete: *https://link.springer.com/book/10.1007/978-3-030-32361-5*.

Massimi M., *Articolo 34 – Comunicazione di una violazione dei dati personali all'interessato*, in E. Belisario, G.M. Riccio, G. Scozza (a cura di), *GDPR e Normativa Privacy*, Milano, 2020, 401-407.

Massimini M., *Anonimizzazione dei dati personali: significato, benefici e dubbi in ottica GDPR*, 2021, in *Privacy.it*, in Rete: *https://www.privacy.it/2021/05/11/anonimizzazione-*

gpdr-massimini/#:~:text=L%27anonimizzazione%20%C3%A8%2C%20come%20detto,tra%20quelle%20elencate%20all%27art.

Mazzamuto S., *Brevi note in tema di mezzi di tutela e di riparto della giurisdizione nelle attività di trattamento dei dati personali*, in V. Cuffaro, V. Ricciuto, V. Zeno Zencovich (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1998, 249-274.

Medzini R., *Governing the shadow of hierarchy: enhanced self-regulation in European data protection codes and certifications*, In *Internet Policy Review*, v. 10(3), 2021, in Rete: *https://doi.org/10.14763/2021.3.1577*.

Monea A., *Regolamento n. 2016/679: la necessità di uno specifico "Modello organizzativo" per la protezione dei dati personali*, in *Azienditalia*, 2019, n. 8-9, 1114-1123.

O'Kane C.P., *Digital privacy and new media: An empirical study assessing the impact of Privacy Seals on personal information disclosure*, Bournemouth, 2019, 77-78, in Rete: *https://eprints.bournemouth.ac.uk/34340/1/O%E2%80%99KANE%2C%20Conor%20Paul_Ph.D._2019.pdf*.

Pedilarco E., *Il mercato unico digitale per l'integrazione europea. La prospettiva del FinTech*, in *MediaLaws*, 2018, n. 3, in Rete: *https://www.medialaws.eu/il-mercato-unico-digitale-per-lintegrazione-europea-la-prospettiva-del-fintech/.*

Pelino E., *Adempimenti per violazioni dei dati personali (c.d. data breach)*, in C. Bistolfi, L. Bolognini, E. Pelino, *Il Regolamento Privacy Europeo*, Milano, 2016, 443-458.

Pennasilico M. (a cura di)., *Manuale di diritto civile dell'ambiente*, Napoli, 2014, 269-274.

Perego M., Persi S., Ponti C., *Il Modello Organizzativo Privacy – MOP*, Torino, 2020.

Pezza F., *Art. 42 - Certificazioni*, in E. Belisario, G.M. Riccio, G. Scozza (a cura di), *GDPR e Normativa Privacy*, Milano, 2020, 475-483.

Pezza F., *Art. 43 – Organismi di certificazione*, in E. Belisario, G.M. Riccio, G. Scozza (a cura di), *GDPR e Normativa Privacy*, Milano, 2020, 484-493.

Pizzetti F. (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018.

Pizzetti F., *La protezione dei dati personali e la sfida dell'intelligenza artificiale*, in F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, 170.

Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali*, Torino, 2016.

Poletti D., Causarano M.C., *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione,* in E. Tosi (a cura di), *Privacy digitale: riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy,* Milano, 2019, 369-416.

Popoli A.R., *Codici di condotta e certificazioni*, in G. Finocchiaro (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, 367-421.

Previti S., Sanzari F., Barchiesi A. (a cura di), *Web reputation e identità aziendale online: strumenti di tutela*, Milano, 2019.

Principato A., *Verso nuovi approcci alla tutela della privacy: privacy by design e privacy default setting*, in *Contratto e impresa*, 2015, n. 1, 197-229.

Proietti G., *Il Digital Services Act: la normativa sui servizi digitali*, in *Diritto Bancario*, 2023, in Rete: *https://www.dirittobancario.it/art/il-digital-services-act-la-normativa-sui-servizi-digitali/*.

Raul A.C., Manoranjan T.D., Mohan V., *United States*, in A.C. Raul (a cura di), *The Privacy, Data Protection and Cybersecurity Law Review*, 2014, 268-294, in Rete: *https://www.sidley.com/-/media/files/publications/2014/11/the-privacy-data-protection-and-cybersecurity-la__/files/united-states/fileattachment/united-states.pdf*.

Resta G., Salerno A., *La responsabilità civile per il trattamento dei dati personali*, in G. ALPA e G. Conte (a cura di), *La responsabilità d'impresa*, Milano, 2015, 643-685.

Rizzini G., *I nodi tra privacy e responsabilità 231 nei rapporti tra soggetti pubblici e privati*, in *Altalex*, 2023, in Rete: *https://www.altalex.com/documents/2023/02/08/nodi-privacy-responsabilita-231-rapporti-soggetti-pubblici-privati*.

Rodrigues R., Barnard-Wills D., Wright D., De Hert P., Papakonstantinou V., Beslay L., Dubois N., *EU Privacy seals project: Inventory and analysis of privacy certification schemes*, 2013, in Rete: *https://data.europa.eu/doi/10.2788/29861*.

Rodrigues R., Wright D., Wadhwa K., *Developing a privacy seal scheme (that works)*, in *International Data Privacy Law*, Vol. 3, Iss. 2, 2013, 100–116, in Rete: *https://doi.org/10.1093/idpl/ips037*.

Rotolo F., *Articolo 32 – Sicurezza del trattamento*, in E. Belisario, G.M. Riccio, G. Scozza (a cura di), *GDPR e Normativa Privacy*, Milano, 2020, 373-384.

Rubinstein I.S., Good N., *The trouble with Article 25 (and how to fix it): the future of data protection by design and default*, in *International Data Privacy Law*, 2020, Vol. 10, No. 1, 37-56, in Rete: *https://doi.org/10.1093/idpl/ipz019*.

Ruohonen J., Mickelsson S., *Reflections on the Data Governance Act*, in *Digital Society (DISO)*, 2, 10, 2023, in Rete: *https://doi.org/10.1007/s44206-023-00041-7*.

Ruotolo G.M., *Le proposte di disciplina di digital services e digital markets della Commissione del 15 dicembre 2020*, in *DPCE Online*, v. 45, n. 4, 2021, 5419-5421, in Rete: *https://www.dpceonline.it/index.php/dpceonline/article/view/1225/1178*.

Savona P., *Il governo del rischio. Diritto dell'incertezza o diritto incerto?*, Napoli, 2013.

Senden L., *Soft Law, Self-Regulation and Co-Regulation in European Law: Where Do They Meet?*, in *Electronic Journal of Comparative Law*, vol. 9.1, 2006, 11.

Sica S., *La responsabilità civile per il trattamento illecito dei dati personali*, in A. Mantelero, D. Poletti (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa, 2018, 161-174.

Sileoni S., *I codici di condotta e le funzioni di certificazione*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I Dati Personali Nel Diritto Europeo*, Torino, 2019, 917-948.

Silvestri P., *Economia. Il codice giuridico del mondo*, in A. Andronico, T. Greco, F. Macioce (a cura di), *Dimensioni del Diritto*, Torino, 2019, 399- 425.

Solove D.J., Schwartz P.M., *ALI Data Privacy: Overview and Black Letter Text*, in *U.C.L.A. Law Review*, 2022, 1252-1300, in Rete: *https://paulschwartz.net/wp-content/uploads/2022/02/Solove-Schwartz-ALI-Data-Privacy-UCLA-L-Rev-2022.pdf*.

Spagnuelo D., Ferreira A., Lenzini G., *Accomplishing Transparency within the General Data Protection Regulation*; in P. Mori, S. Furnell, O. Camp (a cura di), *Proceedings of the 5th International Conference on Information Systems Security and Privacy*, 2019, 114-125, in Rete: *https://pdfs.semanticscholar.org/b1ef/d7ef48255477cfe6d8c81aa613cc18dcd1d0.pdf*.

Documenti dell'European Data Protection Board e delle Autorità Nazionali di Controllo:

Article 29 Data Protection Working Party, *Fablab "GDPR/from concepts to operational toolbox, DIY"- Results of the discussion*, 2017, in Rete: *https://ec.europa.eu/justice/article-29/documentation/other-document/files/2016/20160930_fablab_results_of_discussions_en.pdf*.

Article 29 Data Protection Working Party, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679, WP 248 rev.01*, 2017, in Rete: *https://ec.europa.eu/newsroom/article29/items/611236/en*.

Article 29 Data Protection Working Party, *Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679, WP250rev.01*, 2018, in Rete: *https://ec.europa.eu/newsroom/article29/items/612052*.

Article 29 Data Protection Working Party, *Opinion 1/98 Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)*, 1998, in Rete: *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp11_en.pdf*.

Article 29 Data Protection Working Party, *Parere 3/2010 sul principio di responsabilità, 62/10/IT WP 173*, 2010, in Rete: *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_it.pdf*.

Article 29 Data Protection Working Party, *Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR*, 2018, in Rete: *https://ec.europa.eu/newsroom/article29/items/624045/en*.

Article 29 Data Protection Working Party, *Statement on the role of a risk-based approach in data protection legal frameworks, 14/EN WP 218*, 2014, in Rete: *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf*.

Article 29 Data Protection Working Party, *The future of privacy: joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, 2009, in Rete: *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf*.

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), *The 2022 Activity Report of the Federal Commissioner for Data Protection and Freedom of Information*, 2023, in Rete: *https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Taetigkeitsberichte/31TB_22.pdf?__blob=publicationFile&v=6*.

Commission Nationale Pour La Protection Des Données, *Décision N° 15/2022 - GDPR Certified Assurance Report based Processing Activities Certification Criteria (GDPR-CARPA), V. 1 / 2022*, 2022, in Rete: *https://cnpd.public.lu/dam-assets/fr/professionnels/certification/decision-n-15-2022-du-13-mai-2022-criteres-de-certification.pdf*.

Commission Nationale Pour La Protection Des Données, *Décision N° 8/2020 du 3 avril 2020 de la Commission nationale pour la protection des données portant approbation*

des critères d'agrément des organismes de certification, 2020, in Rete: *https://cnpd.public.lu/content/dam/cnpd/fr/decisions-avis/2020/08-2020-Approbation-criteres-d-agrement-organismes-de-certification-signe.pdf*.

Commission Nationale Pour La Protection Des Données, *GDPR-Certified Assurance Report based Processing Activities Certification Criteria*, 2018, in Rete: *https://cnpd.public.lu/dam-assets/fr/professionnels/certification/GDPR-CARPA-Criteria-for-certification-v10.pdf*.

Commission Nationale Pour La Protection Des Données, *Le schéma de certification "GDPR CARPA"*, 2023, in Rete: *https://cnpd.public.lu/fr/professionnels/outils-conformite/certification/gdpr-carpa.html*.

Commission Nationale Pour La Protection Des Données, *Procédure de la Commission nationale pour la protection des données (CNPD) relative à l'agrément des organismes de certification*, 2021, in Rete: *https://cnpd.public.lu/content/dam/cnpd/fr/professionnels/certification/Procedure-relative-a-l-agrement-des-organismes-de-certification.pdf*.

European Data Protection Board - European Data Protection Supervisor, *Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale)*, 2021, in Rete: *https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_it.pdf*.

European Data Protection Board - European Data Protection Supervisor, *Parere congiunto EDPB-GEPD 2/2022 sulla proposta del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati)*, 2022, in Rete: *https://edpb.europa.eu/system/files/2023-03/edpb-edps_jointopinion_2022-02_data_act_proposal_it.pdf*.

European Data Protection Board, *Documento del Comitato europeo per la protezione dei dati sulla procedura di approvazione da parte del Comitato di criteri di certificazione riferiti a una certificazione comune, il sigillo europeo per la protezione dei dati*, 2020, in Rete: *https://edpb.europa.eu/our-work-tools/our-documents/procedure/edpb-document-procedure-approval-certification-criteria-edpb_it*.

European Data Protection Board, *Guida alla valutazione dei criteri di certificazione – Addendum alle linee guida 1/2018 sulla certificazione e l'identificazione dei criteri di certificazione in conformità agli articoli 42 e 43 del Regolamento*, 2021, in Rete: *https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/Addendum%20Linee%20Guida%201_2018-DEF%20EN.pdf*.

European Data Protection Board, *Linea guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione*

dei dati nel contesto della fornitura di servizi online agli interessati (Vers. 2.0), 2019, in Rete: *https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_it*.

European Data Protection Board, *Linee Guida 1/2018 relative alla certificazione e all'identificazione di criteri di certifica-zione in conformità degli articoli 42 e 43 del Regolamento*, 2019, in Rete: *https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_it.pdf*.

European Data Protection Board, *Linee guida 4/2018 relative all'accreditamento degli organismi di certificazione a norma dell'articolo 43 del regolamento generale sulla protezione dei dati*, 2019, 9, in Rete: *https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_it_0.pdf*.

European Data Protection Board, *Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita*, 2020, in Rete: *https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_it.pdf*.

European Data Protection Board, *Linee guida 7/2022 sulla certificazione come strumento per i trasferimenti*, 2023, in Rete: *https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_07-2022_on_certification_as_a_ tool_ for_transfers_v2_it_0.pdf*.

European Data Protection Board, *Linee-guida 01/2019 sui codici di condotta e sugli organismi di monitoraggio a norma del regolamento (UE) 2016/679*, 2019, in Rete: *https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-0_it*.

European Data Protection Board, *Linee-guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali*, 2022, in Rete: *https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_it*.

European Data Protection Board, *Opinion 1/2022 on the draft decision of the Luxembourg Supervisory Authority regarding the GDPR – CARPA certification criteria*, 2022, in Rete: *https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-12022-draft-decision-luxembourg_en*.

European Data Protection Board, *Opinion 25/2022 regarding the European Privacy Seal (EuroPriSe) certification criteria for the certification of processing operations by processors*, 2022, in Rete: *https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-252022-regarding-european-privacy-seal_en*.

European Data Protection Board, *Parere 23/2020 sul progetto di decisione dell'autorità di controllo competente dell'Italia relativa all'approvazione dei requisiti per l'accreditamento di un organismo di certificazione ai sensi dell'articolo 43, paragrafo 3 (RGPD)*, 2020, in Rete: *https://edpb.europa.eu/system/files/2022-11/edpb_opinion_202023_on_the_it_sa_accreditation_requirements_for_certification_body_it.pdf*.

European Data Protection Board, *Parere 28/2022 sull' approvazione dei criteri di certificazione Europrivacy da parte del Comitato come sigillo europeo per la protezione dei dati a norma dell'articolo 42, paragrafo 5, del regolamento generale sulla protezione dei dati (RGPD)*, 2022, 4, in Rete: *https://edpb.europa.eu/system /files/2023-03/edpb_opinion_202228_europrivacy_eu_data_protection_seal_it.pdf*.

European Data Protection Board, *Statement on the Digital Services Package and Data Strategy*, 2021, in Rete: *https://edpb.europa.eu/system/files/2021-11/edpb_statement_on_the_digital_services_package_and_data_strategy_en.pdf*.

European Data Protection Board, *The CNPD adopts the certification mechanism GDPR-CARPA*, 2022, in Rete: *https://ed pb.euro pa.eu/news/national-news/2022/cnpd-adopts-certification-mechanism-gdpr-carpa_en*.

European Data Protection Supervisor, *Opinion 1/2021 on the Proposal for a Digital Services Act*, 2021, in Rete: *https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_services_act_en.pdf*.

European Data Protection Supervisor, *Opinion 2/2021 on the Proposal for a Digital Markets Act*, 2021, in Rete: *https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_markets_act_en.pdf*.

European Union Agency for Cybersecurity, *Recommendations on European Data Protection Certification*, 2017, in Rete: *https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification*.

Garante per la protezione dei dati personali, *FAQ in materia di accreditamento e certificazione ai sensi del GDPR – parte generale*, in Rete: *https://www.garanteprivacy.it/regolamentoue/certificazione-e-accreditamento.*

Garante per la protezione dei dati personali, *Faq sul Responsabile della Protezione dei Dati (RPD)*, in Rete: *https://www.garanteprivacy.it/faq-sul-responsabile-della-protezione-dei-dati-rpd-in-ambito-privato*.

Garante per la protezione dei dati personali, *Ordinanza di ingiunzione nei confronti di Regione Lazio, registro dei provvedimenti n. 409 dd. 1° dicembre 2022*, in Rete:

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9833530.

Garante per la protezione dei dati personali, *Parere su istanza di accesso civico, registro dei provvedimenti n. 155 dd. 3 settembre 2020*, in Rete: *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9461036*.

Garante per la protezione dei dati personali, *Registro dei provvedimenti n. 396 del 28 giugno 2018*, in Rete: *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9023246*.

Garante per la protezione dei dati personali, *Registro dei provvedimenti n. 348 del 20 ottobre 2022*, in Rete: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9825667.

Garante per la protezione dei dati personali, *Registro dei provvedimenti n. 328 del 6 ottobre 2022*, in Rete: *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9817058*.

Garante per la protezione dei dati personali, *Requisiti di accreditamento "aggiuntivi" dell'Autorità di controllo italiana con riguardo alla norma ISO/IEC 17065:2012 e in conformità dell'articolo 43, paragrafi 1, lettera b) e 3, del Regolamento Generale sulla Protezione dei Dati, registro dei provvedimenti n. 148/2020, 2020, in Rete: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9445086.*

Information Commissioner's Office, *Certification scheme register: ADISA ICT Asset Recovery Certification 8.0*, 2021, in Rete: *https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-scheme-register/adisa-ict-asset-recovery-certification-80/*.

Information Commissioner's Office, *Certification scheme register: Provision of Training and Qualifications Services*, in Rete: *https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-scheme-register/provision-of-training-and-qualifications-services/*.

Information Commissioner's Office, *Certification schemes register: Age Check Certification Scheme (ACCS)*, 2021, in Rete: *https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-scheme-register/age-check-certification-scheme-accs/*.

Information Commissioner's Office, *How do we develop a certification scheme?*, in Rete: *https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-schemes-detailed-guidance/how-do-we-develop-a-certification-scheme/#10*.

Information Commissioner's Office, *Will the ICO consider certification as a mitigating factor in an investigation?*, in Rete: *https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-schemes-detailed-guidance/how-do-we-apply-for-gdpr-certification/#how5*.

Landesbeauftragte für Datenschutz und Informationsfreiheit in NRW, *LDI NRW genehmigt erste deutsche Kriterien für Datenschutz-Zertifizierung*, 2022, in Rete: *https://www.ldi.nrw.de/ldi-nrw-genehmigt-erste-deutsche-kriterien-fuer-datenschutz-zertifizierung*.

Comunicazioni e relazioni delle istituzioni europee

Commissione europea, *COM/2001/428, "La governance europea – Un libro bianco"*, 2001.

Commissione europea, *COM/2010/609, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato Delle Regioni – Un approccio globale alla protezione dei dati personali dell'Unione europea*, 2010, 14, in Rete: *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52010DC0609&from=SK*.

Commissione europea, *COM/2012/0529*, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni: Sfruttare il potenziale del cloud computing in Europa*, 2012, in Rete: *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52012DC0529*.

Commissione europea, *COM/2015/192*, *Comunicazione della Commissione al Parlamento europeo e al Comitato delle regioni, Strategia per il mercato unico digitale in Europa*, 2015.

Commissione europea, *COM/2016/0178*, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni: Iniziativa europea per il cloud computing - costruire un'economia competitiva dei dati e della conoscenza in Europa*, 2016, in Rete: *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=COM:2016:178:FIN*.

Commissione europea, *COM/2020/66, Una strategia europea per i dati,* 2020, in Rete: *https://eur-lex.europa.eu/legal-content/it/txt/?uri=celex%3a52020dc0066*.

Commissione europea, *COM/2021/206, Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione*, 2021, in Rete: *https://eur-lex.europa.eu/legal-content/it/txt/?uri=celex%3a52021pc0206*.

Commissione europea, *COM/2022/68, Proposta di Regolamento del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati)*, 2022, in Rete: *https://eur-lex.europa.eu/legal-content/it/txt/pdf/?uri=celex:52022pc0068*.

Commissione europea, *Commission Implementing Regulation (EU) 2023/4745*, 2023, in Rete: *https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_it*.

Commissione europea, *Comunicato stampa: Protezione dei dati: la Commissione europea adotta una nuova decisione di adeguatezza per la circolazione sicura e affidabile dei flussi di dati UE-USA*, 2023, in Rete: *https://ec.europa.eu/commission/presscorner/detail/it/ip_23_3721*.

Commissione europea, *Data Protection Certification Mechanisms Study on Articles 42 and 43 of the Regulation (EU) 2016/679*, 2019, in Rete: *https://commission.europa.eu/system/files/2019-04/data_protection_certification_mechanisms_study_publish_0.pdf*.

Commissione europea, *DSA: Piattaforme online molto grandi e motori di ricerca*, 2023, in Rete: *https://digital-strategy.ec.europa.eu/it/policies/dsa-vlops*.

Commissione europea, *Europrivacy: the first certification mechanism to ensure compliance with GDPR*, 2022, in Rete: *https://digital-strategy.ec.europa.eu/en/news/europrivacy-first-certification-mechanism-ensure-compliance-gdpr*.

Consiglio dell'Unione europea, *COD/2012/0011*, *Note on Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (GDPR)*, 2013.

Consiglio dell'Unione europea, *Press releases and statements 537/17*, *Remarks by President Donald Tusk after the Tallinn Digital Summit*, 2017, in Rete: *https://www.consilium.europa.eu/en/press/press-releases/2017/09/29/tusk-press-conference-tallinn/*.

Consiglio dell'Unione europea, *Press releases and statements 616/18*, *EU to strengthen sharing of public sector data - Council agrees its position*, 2018, in Rete: *https://www.consilium.europa.eu/en/press/press-releases/2018/11/07/eu-to-strengthen-sharing-of-public-sector-data-council-agrees-its-position/.*

Consiglio d'Europa, *(Convenzione 108) Linee-Guida in materia di intelligenza artificiale e protezione dei dati*, 2019, in Rete: *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9096716*.

European Commission Directorate General for Justice and Consumers, *Glossary in the portal of Justice, definition of privacy by design*, 2015.

Parlamento europeo, Consiglio dell'Unione europea, Commissione europea, *Progetto Interistituzionale - «Legiferare meglio», G.U. 2003/C 321/01*, 2003.

Parlamento europeo, *Relazione A8-0407/2018*, *Relazione del parlamento europeo sulla blockchain: una politica commerciale lungimirante (2018/2085(INI))*, 2018.

Documenti di prassi

Accredia, *Circolare tecnica DC N° 10/2019 – Disposizioni in merito all'accreditamento norma ISO/IEC 27701*, 2019, in Rete: *https://www.accredia.it/documento/circolare-tecnica-dc-n-10-2019-disposizioni-in-merito-allaccreditamento-norma-iso-iec-27701/*.

Cavoukian A., Ryerson University, *Commit to Privacy, Publicly – Privacy by Design Certification Program*, in Rete: *https://www.torontomu.ca/content/dam/pbdce/certification/PbD-Brochure.pdf*.

Centre for Information Policy Leadership, *A Risk-based Approach to Privacy: Improving Effectiveness in Practice*, 2014, in Rete: *https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf*.

Centre for Information Policy Leadership, *Project on Privacy Risk Framework and Risk-based Approach to Privacy*, in Rete: *https://www.informationpolicycentre.com/privacy-risk-management.html*.

Centre for Information Policy Leadership, *Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR*, in *Project on Privacy Risk Framework and Risk-based Approach to Privacy*, 2016, in Rete: *https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf*.

Centre for Information Policy Leadership, *The Role Of Risk Management In Data Protection*, in *Project on Privacy Risk Framework and Risk-based Approach to Privacy*, 2014, in Rete: *https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_2-the_role_of_risk_management_in_data_protection-c.pdf*.

Ciampi C., *Certificazioni in ambito GDPR, ecco il nuovo schema ISDP©10003*, in *CyberSecuriti360*, 2020, in Rete: *https://www.cybersecurity360.it/legal/privacy-dati-personali/certificazioni-in-ambito-gdpr-ecco-il-nuovo-schema-isdp10003/*.

Deloitte, *Privacy by Design Assessment and Certificatio*, in Rete: *https://www.torontomu.ca/content/dam/pbdce/certification/Privacy-by-Design-Overview_PbDCE.pdf*.

Deloitte, *Privacy by Design Certification Program: Assestment Control Framework - Privacy by Design: Privacy Assessment Methodology*, 2016, in Rete: *https://www.torontomu.ca/content/dam/pbdce/certification/Privacy-by-Design-Certification-Program-Assessment-Methodology_PbDCE.pdf.*

European Centre for Certification and Privacy, *Europrivacy GDPR Core Criteria*, 2020, in Rete: *https://community .europrivacy.com/europrivacy-gdpr-core-criteria/*.

European Centre for Certification and Privacy, *Europrivacy Overview*, in Rete: *https://www.europrivacy.org/en/ep/overview*.

EuroPriSe, *EuroPriSe Criteria for certification of IT products and IT-based services*, 2017, in Rete: *https://www.euprivacyseal.com/wp-content/uploads/2023/01/EuroPriSe-Criteria-v201701_final.pdf*

EuroPriSe, *EuroPriSe Criteria for the certification of processing operations by processors*, 2022, in Rete: *https://www.euprivacyseal.com/wp-content/uploads/2022/12/Kriterien_Verarbeitungsvorgange-von-AV_EN_v3_0.pdf*.

EuroPriSe, *EuroPriSe Criteria for the certification of processing operations by processors*, in Rete: *https://www.euprivacyseal.com/certification-schemes/scheme-for-processors/*.

EuroPriSe, *Scheme for IT Products and IT based Services*, in Rete: *https://www.euprivacyseal.com/certification-schemes/scheme-for-products-and-services/*.

Federal Privacy Commision, *Fair Information Practice Principles (FIPPs)*, in Rete: *https://www.fpc.gov/resources/fipps/*.

Federal Trade Commission, *Protecting consumer privacy in an era of rapid change. Recommendations for businesses and policymakers*, 2012, in Rete: *https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf*.

Federprivacy, *Certificazione DPO: i chiarimenti del Garante sulla Norma UNI*, in *Federprivacy*, 2018, in Rete: *https://www.federprivacy.org/attivita/certificazione-dpo-i-chiarimenti-del-garante-sulla-norma-uni*.

Federprivacy, *Cosa è la ISO/IEC 27701?*, in *Federprivacy,* 2019, in Rete: *https://www.federprivacy.org/informazione/sapresti-rispondere/cosa-e-la-iso-iec-27701*.

Giannetti R., *Privacy Day Forum 2023: lo speech di Riccardo Giannetti su Certificazioni & GDPR*, 2023, in Rete: *https://www.youtube.com/watch?v=GmQ7TRvEoqY*.

Impact News Service, *New certification schemes will "raise the bar" of data protection in children's privacy, age assurance and asset disposal*, in LexisNexis, 2021, in Rete: *https://advance.lexis.com/api/document?collection=news&id=urn:contentItem:63F7-2YD1-JDG9-Y46W-00000-00&context=1516831*.

Inveo, *Certificazione ISDP©10003 per la valutazione di conformità al GDPR*, 2020, in Rete: *https://www.in-veo.com/certificazione-isdp-10003-2020-data-protection*.

Inveo, *ISDP©10003, Schema internazionale per la valutazione della conformità al Regolamento Europeo 2016/679*, 2020, in Rete: *https://www.in-veo.com/privacy-tools-new/schema-di-certificazione-isdp-c-10003-dw/37-schema-di-certificazione-isdp-10003-2020-rev-01-ita-new-release*.

Liedekerke, *The European Data Protection Seal as a certification tool*, 2023, in Rete: *https://liedekerke.com/en/insights/the-european-data-protection-seal-as-a-certification-tool*.

Massimini M., *Il registro dei trattamenti GDPR e la deroga fantasma per le PMI*, in *Privacy.it*, 2018, in Rete: *https://www.privacy.it/2018/04/27/massimini-registro-trattamenti-gdpr-deroga/*.

NCSL, *State Laws Related to Digital Privacy*, 2022, in Rete: *https://www.ncsl.org/technology-and-communication/state-laws-related-to-digital-privacy#:~:text=Five%20states%E2%80%94California%2C%20Colorado%2C,of%20personal%20information%2C%20among%20others*.

Perego M., *I nuovi controlli della Norma ISO 27001:2022 che impattano sui dati personali*, in *Federprivacy*, 2022, in Rete: *https://www.federprivacy.org/informazione/primo-piano/i-nuovi-controlli-della-norma-iso-27001-2022-che-impattano-sui-dati-personali*.

Perego M., *La ISO/IEC 27701:2019: la lettura della norma sulla gestione della privacy attraverso le ricorrenze*, in *Federprivacy*, 2022, in Rete: *https://www.federprivacy.org/informazione/primo-piano/la-iso-iec-27701-2019-la-lettura-della-norma-sulla-gestione-della-privacy-attraverso-le-ricorrenze*.

Perego M., *MOP: il Modello Organizzativo Privacy come misura di accountability per la compliance al Gdpr*, in *Federprivacy*, 2022, in Rete:

https://www.federprivacy.org/informazione/primo-piano/mop-il-modello-organizzativo-privacy-come-misura-di-accountability.

Perego M., *Uscita la nuova ISO 27001:2022 con gli standard su sicurezza delle informazioni, cybersecurity e privacy*, in *Federprivacy*, 2022, in Rete: *https://www.federprivacy.org/informazione/primo-piano/uscita-la-nuova-iso-27001-2022-con-gli-standard-su-sicurezza-delle-informazioni-cybersecurity-e-privacy*.

PR Newswire, *European Centre for Certification and Privacy: Europrivacy - The GDPR European Data Protection Seal Approved by the EU, a New Era for Privacy and Data Protection Compliance*, 12 ottobre 2022, in Rete: *https://www.prnewswire.com/news-releases/european-centre-for-certification-and-privacy--europrivacy--the-gdpr-european-data-protection-seal-approved-by-the-eu-a-new-era-for-privacy-and-data-protection-compliance-301647958.html*.

Reisch O., Alexandre D., Dally G., Dehmeche S., *CNPD adopts GDPR-CARPA certification criteria*, in *DLA PIPER – publications*, 2022, in Rete: *https://www.dlapiper.com/en/insights/publications/2022/06/cnpd-adopts-gdpr-carpa-certification-criteria*.

Riccio G.M., Viti V., *Le "Certificazioni privacy" ed il Regolamento UE*, in *MediaLaws*, 2017, in Rete: *https://www.medialaws.eu/le-certificazioni-privacy-ed-il-regolamento-ue/.*

Salvi M.A., *Certificazioni privacy e certificazioni GDPR: quali sono e perché non sono la stessa cosa*, in *Cybersecurity360*, 2021, in Rete: *https://www.cybersecurity360.it/legal/privacy-dati-personali/certificazioni-privacy-e-certificazioni-gdpr-quali-sono-e-perche-non-sono-la-stessa-cosa/*.

Somers G., Gryffroy P., *The first EU-wide GDPR Certification Scheme – Europrivacy (Tm/®) explained in 5 questions*, in *Timelex*, 2022, in Rete: *https://www.timelex.eu/en/europrivacy*.

Sookman B., *Privacy by Design certification framework launched by Ryerson and Deloitte*, 2015, in Rete: *https://www.barrysookman.com/2015/05/25/privacy-by-design-certification-framework-launched-by-ryerson-and-deloitte/*.

Tevere V., *Coronavirus: soggetti contagiati e profili di riservatezza - Garante Privacy, provvedimento n. 155/2020: è ammissibile un'istanza di accesso generalizzato ai dati concernenti la salute di soggetti contagiati da Covid-19?,* in *Altalex*, 2020, in Rete: *https://www.altalex.com/documents/news/2020/10/29/coronavirus-soggetti-contagiati-profili-riservatezza.*

TrustArc Inc, *TRUSTe APEC Privacy Certification Standards*, 2016, in Rete: *https://download.trustarc.com/dload.php/?f=LH7RIJRS-627*.

U.S. Department of Commerce, *Data Privacy Framework Principles: 1. Notice*, in Rete: *https://www.dataprivacyframework.gov/s/article/1-notice-dpf?tabset-35584=2*.

U.S. Department of Commerce, *Data Privacy Framework Principles: 2. Choice*, in Rete: *https://www.dataprivacyframework.gov/s/article/2-choice-dpf?tabset-35584=2*.

U.S. Department of Commerce, *Data Privacy Framework Principles: 3. Accountability for onward transfer*, in Rete: *https://www.dataprivacyframework.gov/s/article/3-accountability-for-onward-transfer-dpf?tabset-35584=2*.

U.S. Department of Commerce, *Data Privacy Framework Principles: 4. Security*, in Rete: *https://www.dataprivacyframework.gov/s/article/4-security-dpf?tabset-35584=2*.

U.S. Department of Commerce, *Data Privacy Framework Principles: 5. Data integrity and purpose limitation*, in Rete: *https://www.dataprivacyframework.gov/s/article/5-data-integrity-and-purpose-limitation-dpf?tabset-35584=2*.

U.S. Department of Commerce, *Data Privacy Framework Principles: 6. Access*, in Rete: *https://www.dataprivacyframework.gov/s/article/6-access-dbf?tabset-35584=2*.

U.S. Department of Commerce, *Data Privacy Framework Principles: 7. Recourse, enforcement and liability*, in Rete: *https://www.dataprivacyframework.gov/s/article/7-recourse-enforcement-and-liability-dpf?tabset-35584=2*.

U.S. Department of Commerce, *How to Join the Data Privacy Framework (DPF) Program (part 1)*, in Rete: *https://www.dataprivacyframework.gov/s/article/how-to-join-the-data-privacy-framework-dpf-program-part-1-dpf?tabset-35584=1*.

U.S. Department of Commerce, *How to Join the Data Privacy Framework (DPF) Program (part 2)*, in Rete: *https://www.dataprivacyframework.gov/s/article/how-to-join-the-data-privacy-framework-dpf-program-part-2-dpf*.

UNI, *Una terminologia comune per la sicurezza delle informazioni*, 2016, in Rete: *https://www.uni.com/index.php?option=com_content&view=article&id=4686:una-terminologia-comune-per-la-sicurezza-delle-informazioni&catid=171:istituzionale&Itemid=2612#.*

Fonti normative

Trattato di Maastricht, del 7 febbraio 1992 (GU C 191 del 29.07.1992).

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 (GU C 281 del 23.11.1995).

Decreto Legislativo 30 giugno 2003, n.196 recante il “Codice in materia di protezione dei dati personali”, integrato con le modifiche introdotte dal Decreto Legislativo 10 agosto 2018, n. 101, recante “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679.

Trattato di Lisbona del 13 dicembre 2007 (GU C 306 del 17.12.2007).

Regolamento. (CE) N. 765/2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti.

Carta dei Diritti Fondamentali dell’Unione europea (GU C 202 del 07.06.2016).

Regolamento (EU) 2016/679 del Parlamento europeo 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 (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 Maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati), 2022, in Rete: *https://eur-lex.europa.eu/legal-content/it/txt/html/?uri=celex:32022r0868*.

Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali), in Rete: *https://eur-lex.europa.eu/legal-content/it/txt/pdf/?uri=celex:32022r1925&qid=1691450780883*.

Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), in Rete: *https://eur-lex.europa.eu/legal-content/it/txt/pdf/?uri=celex:32022r2065*.

The Student Paper Series of the Trento LawTech Research Group is published since 2010

https://lawtech.jus.unitn.it/main-menu/paper-series/student-paper-series-of-the-trento-lawtech-research-group/2/

Freely downloadable papers already published:

STUDENT PAPER N. 90

La didattica del capitalismo della sorveglianza: profili giuridici

ALICE CATALANO. La didattica del capitalismo della sorveglianza: profili giuridici. Trento Law and Technology Research Group, Student Paper Series; 90. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 89

Il «danno da movida» tra tutela inibitoria e risarcimento del danno

ANNALIA MAISTRELLI. Il «danno da movida» tra tutela inibitoria e risarcimento del danno. Trento Law and Technology Research Group, Student Paper Series; 89. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 88

Disvelamento dei fatti e responsabilità civile: la funzione sociale del giornalismo d'inchiesta e del whistleblowing

ALBERTO SCANDOLA. Disvelamento dei fatti e responsabilità civile: la funzione sociale del giornalismo d'inchiesta e del whistleblowing. Trento Law and Technology Research Group, Student Paper Series; 88. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 87

Responsabilità e accountability in materia di protezione dei dati personali: il contesto dell'internet of things

ANDREA BLATTI. Responsabilità e accountability in materia di protezione dei dati personali: il contesto dell'internet of things. Trento Law and Technology Research Group, Student Paper Series; 87. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 86

Il capitalismo dei monopoli intellettuali e l'editoria della sorveglianza. un'analisi delle politiche europee sull'open science e sulla regolazione dei dati

CAMILLA FRANCH. Il capitalismo dei monopoli intellettuali e l'editoria della sorveglianza. un'analisi delle politiche europee sull'open science e sulla regolazione dei dati. Un'analisi critica. Trento Law and Technology Research Group, Student Paper Series; 86. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 85

Transformative Agreements: i nuovi contratti tra editori scientifici e istituzioni accademiche per l'accesso alle risorse scientifiche digitali. Un'analisi critica

MIRIANA FIERRO. Transformative Agreements: i nuovi contratti tra editori scientifici e istituzioni accademiche per l'accesso alle risorse scientifiche digitali. Un'analisi critica. Trento Law and Technology Research Group, Student Paper Series; 85. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 84

La blockchain, tra prorietà e proprietà intellettuale. Analisi comparata di tre applicazioni nel diritto civile

NICOLÒ CANAL. La blockchain, tra prorietà e proprietà intellettuale. Analisi comparata di tre applicazioni nel diritto civile. Trento Law and Technology Research Group, Student Paper Series; 84. Trento: Università degli Studi di Trento.

STUDENT PAPER N.83

La ricerca di un criterio di quantificazione tipologico per il danno da perdita di chance nella responsabilità medica: una missione impossibile?

VALERIA LUCCARINI. La ricerca di un criterio di quantificazione tipologico per il danno da perdita di chance nella responsabilità medica: una missione impossibile. Trento Law and Technology Research Group, Student Paper Series; 83. Trento: Università degli Studi di Trento.

STUDENT PAPER N.82

La responsabilità civile da deficit organizzativo del sistema sanitario e l'emergenza pandemica: una comparazione fra Germania e Italia

JESSICA RIVA**.** La responsabilità civile da deficit organizzativo del sistema sanitario e l'emergenza pandemica: una comparazione fra Germania e Italia. Trento Law and

Technology Research Group, Student Paper Series; 82. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 81

La vaccinazione infausta fra tutela indennitaria e risarcitoria: infausta fra tutela indennitaria e risarcitoria: la gestione del danno da vaccino dopo la pandemia

VERONICA MAYRHOFER. La vaccinazione infausta fra tutela indennitaria e risarcitoria: la gestione del danno da vaccino dopo la pandemia, Trento Law and Technology Research Group, Student Paper Series; 81. Trento: Università degli Studi di Trento

STUDENT PAPER N. 80

La responsabilità civile per i veicoli a guida autonoma nell'ordinamento tedesco: spunti per il legislatore italiano

ELENA TOGNON, La responsabilità civile per i veicoli a guida autonoma nell'ordinamento tedesco: spunti per il legislatore italiano, Trento Law and Technology Research Group, Student Paper Series; 80. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 79

La tutela delle indicazioni geografiche per i prodotti non comparabili: il ruolo dei gruppi di produttori nella valorizzazione del segno

MARTINA DURIGON, La tutela delle indicazioni geografiche per i prodotti non comparabili: il ruolo dei gruppi di produttori nella valorizzazione del segno, Trento Law and Technology Research Group, Student Paper Series; 79. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 78
Il diritto alle prese con la vulnerabilità del turismo, fra guerra e persistente pandemia

FRANCESCA ROMANA BARBA; GIACOMO MARTINO BELLUZZO; SEBASTIANO BORILE; MATTEO BUDELLINI; CHIARA BUOSI; WIKTOR BURIGO; PAOLO CAPOTI; SERENA CARRUBBA; ALESSANDRA CASAGRANDE; FEDERICO DE VINCENZO; EMILIA FASCINELLI; CATERINA FAVA; ANTONIO FERRARO; CAROLINA FILICE; ALESSIA GIZZARELLI; ARIANNA LANEVE; MATTIA LEONE; MARTINA LUCE; MATTEO MAIOLI; 227 ALESSANDRO MARRAS; SARA MATTÈ; ILARIA MELCHIORETTO; ALESSIO MIRA; GIULIA MOCANU; DANIELA NESPOLO; ALESSANDRO OLIVA; ELENA PAGLIAI; ALESSANDRO PALLAORO; SILVIA PEDROTTI; GIACOMO PILI; ALFIO RACITI; FRANCESCA RIZZI, SARA ROSSO; SARA SCARAMUZZA; MARTINO SERAFINI; ELISA SERVIDIO; DENIS SOMMARIVA; CAROLA

STEFENELLI; MARTINA TADDEI; JENNY TURRIN (2022), Trento Law and Technology Research Group, Student Paper Series; 78. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 77

L'enforcement del diritto d'autore e la tutela dei dati personali: il nuovo art. 17 Dir. 2019/790

NICCOLÒ BULLATO, L'enforcementdel diritto d'autore e la tutela dei dati personali: il nuovo art. 17 Dir. 2019/790, Trento Law and Technology Research Group, Student Paper Series; 77. Trento: Università degli Studi di Trento.
https://doi.org/10.5281/zenodo.6630507

STUDENT PAPER N. 76

Il binomio «sport e salute» nella riforma del diritto dello sport: istituzioni, strutture, professionalità e responsabilità

NICOLA INTRONA (2022), Il binomio «sport e salute» nella riforma del diritto dello sport: istituzioni, strutture, professionalità e responsabilità, Trento Law and Technology Research Group, Student Paper Series; 76. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 75

La libertà di panorama: profili critici e spunti comparatistici

CAROLINA BATTISTELLA (2022), La libertà di panorama: profili critici e spunti comparatistici, Trento Law and Technology Research Group, Student Paper Series; 75. Trento: Università degli Studi di Trento. DOI: 10.5281/zenodo.639300

STUDENT PAPER N. 74

The role of copyright in innovation: a comparative analysis of the legal framework of text and data mining

EUGENIO DE BIASI (2022), The role of copyright in innovation: a comparative analysis of the legal framework of text and data mining, Trento Law and Technology Research Group, Student Paper Series; 74. Trento: Università degli Studi di Trento. DOI: 10.5281/ZENODO.5897183

STUDENT PAPER N. 73

Risarcimento del danno da violazione dei diritti di proprietà intellettuale e retroversione degli utili. Un'analisi comparata

FEDERICO BRUNO (2022), Risarcimento del danno da violazione dei diritti di proprietà intellettuale e retroversione degli utili. Un'analisi comparata, Trento Law and Technology Research Group, Student Paper Series; 73. Trento: Università degli Studi di Trento. DOI: 10.5281/zenodo.5878282

STUDENT PAPER N. 72

Eccezioni e limitazioni al diritto d'autore nell'Unione europea: profili critici e spunti comparatistici applicati al settore GLAM alla luce dell'emergenza Covid-19

ELEONORA MARONI (2021), Eccezioni e limitazioni al diritto d'autore nell'Unione europea: profili critici e spunti comparatistici applicati al settore GLAM alla luce dell'emergenza Covid-19, Trento Law and Technology Research Group, Student Paper Series; 72. Trento: Università degli Studi di Trento. DOI:10.5281/zenodo.587821

STUDENT PAPER N. 71

L'*animal welfare* nelle filiere alimentari: etichettatura e certificazioni

ZANON MIRIANA (2021), L'*animal welfare* nelle filiere alimentari: etichettatura e certificazioni, Trento Law and Technology Research Group, Student Paper Series; 71. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-959-8

STUDENT PAPER N. 70

Aggiornamenti di diritto agroalimentare nella riflessione dottrinale angloamericana

ANADOTTI, ELENA; DI GIOVANNI, SILVIA; FREZZA, ANNA CAROLINA; HOSSU, LORENA PATRICIA; MARCONATO, ELENA; NOSCHESE, ANGELA; PENDENZA, ALICE; PEPE, FRANCESCO; PIEROBON, VALERIA; POLI, ELISA; PURITA, CLAUDIA; RAFFA, DJAMILA; ROTONDI, SERGIO ANDREA; SANTOLIN, GAIA – a cura di IZZO, UMBERTO; FERRARI, MATTEO (2021), Aggiornamenti di diritto agroalimentare nella riflessione dottrinale angloamericana, Trento Law and Technology Research Group, Student Paper Series; 70. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-958-1

STUDENT PAPER N. 69

Diritto del turismo e Covid-19: cosa è cambiato nella seconda estate pandemica

ANGIARI, YOUSSEF; ARZARELLO, ANDREA; AZILI, FEDERICO; BONOMELLI, CHIARA; BUBBOLA, IRENE; CADAMURO, CLAUDIA; CARRETTA, ANNA; CONDOTTA, ALESSANDRO; DA PRATO, MARIKA; DAL TOSO, VIRGINIA; DE AGOSTINI, FILIPPO; DE FRANCESCHI, SERENA; DELL'EVA, MARTINA; DELMARCO, MARTINA; DELLA MURA, MARCO; DI MASCIO, FRANCESCA; FIUTEM, LORENZO; GENNARA, GIULIA; INNOCENTI, ALBERTO; LORIERI, ANNA; MAFFEI, BEATRICE; MARCOLINI, ALESSIA; MANZO, ARIANNA;

MINERVINI, MONICA MARIA; MURESAN, ANAMARIA ELENA; NARDIN, NICOLÒ; PAISSAN, FILIPPO; PAISSAN, INGMAR; PANERO, MARTINA; PAVALEANU, CRISTIAN; RIZ, FRANCESCA; SCARSELLA, ALESSIA; SCODANIBBIO, GIULIA; SORRENTINO, MARIAROSA; TUCCI, GIULIANA; VIGNOLI, MARTINA; ZACCARIN, STEPHANIE; ZUCAL, SARA; IZZO, UMBERTO (a cura di) (2021), Diritto del turismo e Covid-19: cosa è cambiato nella seconda estate pandemica, Trento Law and Technology Research Group, Student Paper Series; 69. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-954-3

STUDENT PAPER N. 68

La protezione dei dati relativi alla salute nell'era dei Big Data. Un'analisi sulla sanità digitale in dialogo tra diritto e tecnologia

LIEVORE ANNA (2021), La protezione dei dati relativi alla salute nell'era dei Big Data. Un'analisi sulla sanità digitale in dialogo tra diritto e tecnologia, Trento Law and Technology Research Group, Student Paper Series; 68. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-903-1

STUDENT PAPER N. 67

«Cuius commoda, eius et incommoda»: l'art. 2049 del codice civile nella gig economy

PILZER LARA (2021), «Cuius commoda, eius et incommoda»: l'art. 2049 del codice civile nella gig economy, Trento Law and Technology Research Group, Student Paper Series; 67. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-946-8

STUDENT PAPER N. 66

La responsabilità sanitaria nel post Covid-19: scenari e proposte per affrontare il contenzioso

PRIMICERI GIORGIA (2021), La responsabilità sanitaria nel post Covid-19: scenari e proposte per affrontare il contenzioso, Trento Law and Technology Research Group, Student Paper Series; 66. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-945-1

STUDENT PAPER N. 65

Legal design e sanità digitale: un innovativo approccio per favorire la tutela dei dati personali

FRANCESCO TRAVERSO (2021), Legal design e sanità digitale: un innovativo approccio per favorire la tutela dei dati personali, Trento Law and Technology Research Group, Student Paper Series; 65. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-943-7

STUDENT PAPER N. 64

Sistemi decisionali automatizzati e tutela dei diritti: tra carenza di trasparenza ed esigenze di bilanciamento

IRENE TERENGHI (2021), Sistemi decisionali automatizzati e tutela dei diritti: tra carenza di trasparenza ed esigenze di bilanciamento, Trento Law and Technology Research Group. Student Paper Series; 64. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-942-0

STUDENT PAPER N. 63

Il disegno industriale e la moda tra disciplina dei disegni e modelli e normativa sul diritto d'autore

RUDIAN, MARGHERITA (2021), Il disegno industriale e la moda tra disciplina dei disegni e modelli e normativa sul diritto d'autore, Trento Law and Technology Research Group. Student Paper Series; 63. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-941-3

STUDENT PAPER N. 62

L'appropriazionismo artistico nell'arte visual: una comparazione tra Italia e Stati Uniti

DI NICOLA, LAURA (2021), L'appropriazionismo artistico nell'arte visual: una comparazione tra Italia e Stati Uniti, Trento Law and Technology Research Group. Student Paper Series; 62. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-940-6

STUDENT PAPER N. 61

Unfair trading practices in the business-to-business food supply chain between public and private regulation

BORGHETTO, MARIA VITTORIA (2020), Unfair trading practices in the business-to-business food supply chain between public and private regulation, Trento Law and Technology Research Group. Student Paper Series; 61. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-933-8

STUDENT PAPER N. 60

PFAS e inquinamento delle falde acquifere venete: la tutela civilistica fra danno ambientale e azioni risarcitorie collettive

RAISA, VERONICA (2020), PFAS e inquinamento delle falde acquifere venete: la tutela civilistica fra danno ambientale e azioni risarcitorie collettive, Trento Law and Technology Research Group. Student Paper Series; 60. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-927-7

STUDENT PAPER N. 59

Il turismo alla prova del covid-19: una ricerca interdisciplinare: da quali dati partire e quali risposte dare alla più grande crisi che il comparto turistico abbia mai affrontato

UMBERTO IZZO (a cura di), Autori: ANDREATTA, GIULIA; ANDREOLI, ELISA; ARDU, SIMONE; BORTOLOTTO, FABIO; BRUZZO, PIERLUIGI; CALZOLARI, GIULIA; CAMPOS SANTOS, DIEGO; CARLINO, PIETRO; CAVALLERA, LORENZO; CEPPAROTTI, GIACOMO; CIABRELLI, ANTONIA; DALLE PALLE, GIORGIA; DAPRÀ, VALENTINA; DE SANTIS, DIEGO; FAVARO, SILVIA; FAVERO, ELEONORA; FERRARI, LAURA; GATTI, VERONICA; GAZZI, CHRISTIAN; GISMONDO, MARIANNA; GIUDICEANDREA, ANNA; GUIDA, GIOVANNI; INCARNATO, ANDREA; MARANER, ROBERTA; MICHELI, MARTA; ELENA MORARASU, LAURA; CHIARA NARDELLI, MARIA; PALLOTTA, EMANUELE; PANICHI, NICCOLÒ; PELLIZZARI, LAURA; PLAKSII, ANDRII; RANIERO, SAMANTHA; REGNO SIMONCINI, EMANUELE; RUSSO, SARA; SCHIAVONE, SARA; SERAFINO, ANTONIO; SILENZI, LUCA; TIRONZELLI, ELENA; PEGGY TSAFACK, CYNTHIA; VIGLIOTTI, AYLA; ZINETTI, GIULIA, Il turismo alla prova del Covid-19: una ricerca interdisciplinare: da quali dati partire e quali risposte dare alla più grande crisi che il comparto turistico abbia mai affrontato, Trento Law and Technology Research Group, Student Paper Series; 59. Trento: Università degli Studi di Trento. 978-88-8443-903-1

STUDENT PAPER N. 58

La responsabilità dell'internet service provider alla luce della nuova direttiva sul diritto d'autore nel mercato unico digitale

CAMARELLA, LAURA (2020), La responsabilità dell'Internet Service Provider alla luce della nuova direttiva sul diritto d'autore nel mercato unico digitale, Student Paper Series; 58. Trento: Università degli Studi di Trento. 978-88-8443-893-5

STUDENT PAPER N. 57

Rischio idrogeologico e responsabilità civile

ROBERTI, CATERINA (2020), Rischio idrogeologico e responsabilità civile, Trento Law and Technology Research Group. Student Paper Series; 57. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-891-1

STUDENT PAPER N. 56

Assistente vocale e dati sanitari. Le sfide dell'intelligenza artificiale alla luce del Regolamento (UE) n. 2016/679

PETRUCCI, LIVIA (2020), Assistente vocale e dati sanitari. Le sfide dell'intelligenza artificiale alla luce del regolamento (UE) N. 2016/679, Trento Law and Technology Research Group. Student Paper Series; 56. Trento: Università degli Studi di Trento. ISBN: 978 88 8443 888 1

STUDENT PAPER N. 55

The Legal Dimension of Energy Security in EU Law

SCHMIEDHOFER, ANDREAS (2020), The legal dimensions of energy security in EU law, Trento Law and Technology Research Group. Student Paper Series; 55. Trento: Università degli Studi di Trento. ISBN: 978 88 8443 888 1

STUDENT PAPER N. 54

Macchine intelligenti che creano ed inventano. Profili e rilievi critici del nuovo rapporto tra intelligenza artificiale e diritti di proprietà intellettuale

TREVISANELLO, LAURA (2020), Macchine intelligenti che creano ed inventano. Profili e rilievi critici del nuovo rapporto tra intelligenza artificiale e diritti di proprietà intellettuale, Trento Law and Technology Research Group. Student Paper Series; 54. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-887-4

STUDENT PAPER N. 53

La protezione delle indicazioni geografiche: il sistema europeo e il sistema cinese a confronto

COGO, MARTA (2019), La protezione delle indicazioni geografiche: il sistema europeo e il sistema cinese a confront, Trento Law and Technology Research Group. Student Paper Series; 53. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-856-0

STUDENT PAPER N. 52

Responsabilità civile e prevenzione dell'abuso interpersonale, fra molestie sessuali e bullismo

PERETTI, FRANCESCA (2019), Responsabilità civile e prevenzione dell'abuso interpersonale, fra molestie sessuali e bullismo, Trento Law and Technology Research Group. Student Paper Series; 52. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-856-0

STUDENT PAPER N. 51

Blockchain, Smart Contract e diritto d'autore nel campo della musica

FAGLIA, FRANCESCO (2019), Blockchain, Smart Contract e diritto d'autore nel campo della musica, Trento Law and Technology Research Group. Student Paper Series; 51. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-855-3

STUDENT PAPER N. 50

Regole per l'innovazione: responsabilità civile e assicurazione di fronte all'auto a guida (progressivamente) autonoma

ZEMIGNANI, FILIPPO (2019), Regole per l'innovazione: responsabilità civile e assicurazione di fronte all'auto a guida (progressivamente) autonoma, Trento Law and Technology Research Group. Student Paper Series; 50. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-850-8

STUDENT PAPER N. 49

Unravelling the nexus between food systems and climate change: a legal analysis. A Plea for smart agriculture, a "new" organic agriculture and a wiser use of biotechnologies in the name of human rights protection

TELCH, ALESSANDRA (2019), Unravelling the nexus between food systems and climate change: a legal analysis. A Plea for smart agriculture, a "new" organic agriculture and a wiser use of biotechnologies in the name of human rights protection, Trento Law and Technology Research Group. Student Paper Series; 49. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-842-3

STUDENT PAPER N. 48

Wireless community networks e responsabilità extracontrattuale

VIDORNI, CHIARA (2019), Wireless community networks e responsabilità extracontrattuale, Trento Law and Technology Research Group. Student Paper Series; 48. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-841-6

STUDENT PAPER N. 47

Proprietà intellettuale e scienza aperta: il caso studio del Montreal Neurological Institute

CASSIN, GIOVANNA (2019), Proprietà intellettuale e scienza aperta: il caso studio del Montreal Neurological Institute, Trento Law and Technology Research Group. Student Paper Series; 47. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-835-5

STUDENT PAPER N. 46

Il "ciclista previdente" che si scontrò due volte: con un'auto e col principio indennitario applicato all'assicurazione infortuni

CHRISTOPH SIMON THUN HOHENSTEIN WELSPERG (2019), Il "ciclista previdente" che si scontrò due volte: con un'auto e col principio indennitario applicato all'assicurazione infortuni, Trento Law and Technology Research Group. Student Paper Series; 46. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-834 8

STUDENT PAPER N. 45

«Errare humanum est». L'errore nel diritto tra intenzionalità, razionalità ed emozioni

BENSALAH, LEILA (2018), «Errare humanum est». L'errore nel diritto tra intenzionalità, razionalità ed emozioni, Trento Law and Technology Research Group. Student Paper Series; 45. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-829-4

STUDENT PAPER N. 44

La gestione del rischio fitosanitario nel diritto agroalimentare europeo ed italiano: il caso Xylella

DE NOBILI, MARINA (2018), La gestione del rischio fitosanitario nel diritto agroalimentare europeo ed italiano: il caso Xylella, Trento Law and Technology Research Group. Student Paper Series; 44. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-828-7

STUDENT PAPER N. 43

Mercato agroalimentare e disintermediazione: la dimensione giuridica della filiera corta

ORLANDI, RICCARDO (2018), Mercato agroalimentare e disintermediazione: la dimensione giuridica della filiera corta, Trento Law and Technology Research Group. Student Paper Series; 43. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-827-0

STUDENT PAPER N. 42

Causa, meritevolezza degli interessi ed equilibrio contrattuale

PULEJO, CARLO ALBERTO (2018), Causa, meritevolezza degli interessi ed equilibrio contrattuale, Trento Law and Technology Research Group. Student Paper Series; 42. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-810-2

STUDENT PAPER N. 41

Graffiti, street art e diritto d'autore: un'analisi comparata

GIORDANI, LORENZA (2018), Graffiti, street art e diritto d'autore: un'analisi comparata, Trento Law and Technology Research Group. Student Paper Series; 41. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-809-6

STUDENT PAPER N. 40

Volo da diporto o sportivo e responsabilità civile per l'esercizio di attività pericolose

MAESTRINI, MATTIA (2018), Volo da diporto o sportivo e responsabilità civile per l'esercizio di attività pericolose, Trento Law and Technology Research Group. Student Paper Series; 40. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-784-6

STUDENT PAPER N. 39

"Attorno al cibo". Profili giuridici e sfide tecnologiche dello Smart Packaging in campo alimentare

BORDETTO, MATTEO (2018), "Attorno al cibo". Profili giuridici e sfide tecnologiche dello Smart Packaging in campo alimentare, Trento Law and Technology Research Group. Student Paper Series; 39. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-795-2

STUDENT PAPER N. 38

Kitesurf e responsabilità civile

RUGGIERO, MARIA (2018), Kitesurf e responsabilità civile, Trento Law and Technology Research Group. Student Paper Series; 38. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-793-8

STUDENT PAPER N. 37

Giudicare e rispondere. La responsabilità civile per l'esercizio della giurisdizione in Italia, Israele e Spagna

MENEGHETTI HISKENS, SARA (2017), Giudicare e rispondere. La responsabilità civile per l'esercizio della giurisdizione in Italia, Israele e Spagna, Trento Law and Technology Research Group. Student Paper Series; 37. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-778-5

STUDENT PAPER N. 36

Il diritto in immersione: regole di sicurezza e responsabilità civile nella subacquea

CAPUZZO, MARTINA (2017), Il diritto in immersione: regole di sicurezza e responsabilità civile nella subacquea, Trento Law and Technology Research Group. Student Paper Series; 36. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-775-4

STUDENT PAPER N. 35

La privacy by design: un'analisi comparata nell'era digitale

BINCOLETTO, GIORGIA (2017), La privacy by design: un'analisi comparata nell'era digitale, Trento Law and Technology Research Group. Student Paper Series; 35. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-733-4

STUDENT PAPER N. 34

La dimensione giuridica del Terroir

BERTINATO, MATTEO (2017), La dimensione giuridica del Terroir, Trento Law and Technology Research Group. Student Paper Series; 34. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-728-0

STUDENT PAPER N. 33

La gravità del fatto nella commisurazione del danno non patrimoniale: un'indagine (anche) nella giurisprudenza di merito

MARISELLI, DAVIDE (2017), La gravità del fatto nella commisurazione del danno non patrimoniale: un'indagine (anche) nella giurisprudenza di merito, Trento Law and Technology Research Group. Student Paper Series; 33. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-727-3

STUDENT PAPER N. 32

«Edible insects». L'Entomofagia nel quadro delle nuove regole europee sui novel foods

TASINI, FEDERICO (2016), «Edible insects». L'Entomofagia nel quadro delle nuove regole europee sui novel foods = «Edible Insects»: Entomophagy in light of the new European

Legislation on novel Foods, Trento Law and Technology Research Group. Student Paper Series; 32. Trento: Università degli Studi di Trento. ISBN 978-88-8443-709-9

STUDENT PAPER N. 31

L'insegnamento dello sci: responsabilità civile e assicurazione per danni ad allievi o a terzi

TAUFER FRANCESCO (2016), L'insegnamento dello sci: responsabilità civile e assicurazione per danni ad allievi o a terzi, Trento Law and Technology Research Group. Student Paper Series; 31. Trento: Università degli Studi di Trento. ISBN 978-88-8443-697-9

STUDENT PAPER N. 30

Incrocio tra Contratti e Proprietà Intellettuale nella Innovazione Scientifica e tecnologica: il Modello del Consortium Agreement europeo

MAGGIOLO ANNA (2016), Incrocio tra Contratti e Proprietà Intellettuale nella Innovazione Scientifica e tecnologica: il Modello del Consortium Agreement europeo, Trento Law and Technology Research Group. Student Paper Series; 30. Trento: Università degli Studi di Trento. ISBN 978-88-8443-696-2

STUDENT PAPER N. 29

La neutralità della rete

BIASIN, ELISABETTA (2016) La neutralità della rete, Trento Law and Technology Research Group. Student Paper Series; 29. Trento: Università degli Studi di Trento. ISBN 978-88-8443-693-1

STUDENT PAPER N. 28

Negotiation Bases and Application Perspectives of TTIP with Reference to Food Law

ACERBI, GIOVANNI (2016) Negotiation Bases and Application Perspectives of TTIP with Reference to Food Law. The Trento Law and Technology Research Group. Student Paper Series; 28. Trento: Università degli Studi di Trento. ISBN 978-88-8443-563-7

STUDENT PAPER N. 27

Privacy and Health Data: A Comparative analysis

FOGLIA, CAROLINA (2016) Privacy and Health Data: A Comparative analysis. The Trento Law and Technology Research Group. Student Paper Series; 27. Trento: Università degli Studi di Trento. ISBN 978-88-8443-546-0

STUDENT PAPER N. 26

Big Data: Privacy and Intellectual Property in a Comparative Perspective

SARTORE, FEDERICO (2016) Big Data: Privacy and Intellectual Property in a Comparative Perspective. The Trento Law and Technology Research Group. Student Paper Series; 26. Trento: Università degli Studi di Trento. ISBN 978-88-8443-534-7

STUDENT PAPER N. 25

Leggere (nel)la giurisprudenza: 53 sentenze inedite in tema di responsabilità civile nelle analisi di 53 annotatori in formazione = Reading (in) the caselaw: 53 unpublished judgemnts dealing with civil liability law analyzed with annotations and comments by 53 students during their civil law course

REMO ANDREOLLI, DALILA MACCIONI, ALBERTO MANTOVANI, CHIARA MARCHETTO, MARIASOLE MASCHIO, GIULIA MASSIMO, ALICE MATTEOTTI, MICHELE MAZZETTI, PIERA MIGNEMI, CHIARA MILANESE, GIACOMO MINGARDO, ANNA LAURA MOGETTA, AMEDEO MONTI, SARA MORANDI, BENEDETTA MUNARI, EDOARDO NADALINI, SERENA NANNI, VANIA ODORIZZI, ANTONIA PALOMBELLA, EMANUELE PASTORINO, JULIA PAU, TOMMASO PEDRAZZANI, PATRIZIA PEDRETTI, VERA PERRICONE, BEATRICE PEVARELLO, LARA PIASERE, MARTA PILOTTO, MARCO POLI, ANNA POLITO, CARLO ALBERTO PULEJO, SILVIA RICCAMBONI, ROBERTA RICCHIUTI, LORENZO RICCO, ELEONORA RIGHI, FRANCESCA RIGO, CHIARA ROMANO, ANTONIO ROSSI, ELEONORA ROTOLA, ALESSANDRO RUFFINI, DENISE SACCO, GIULIA SAKEZI, CHIARA SALATI, MATTEO SANTOMAURO, SILVIA SARTORI, ANGELA SETTE, BIANCA STELZER, GIORGIA TRENTINI, SILVIA TROVATO, GIULIA URBANIS, MARIA CRISTINA URBANO, NICOL VECCARO, VERONICA VILLOTTI, GIULIA VISENTINI, LETIZIA ZAVATTI, ELENA ZUCCHI (2016) Leggere (nel)la giurisprudenza: 53 sentenze inedite in tema di responsabilità civile nelle analisi di 53 annotatori in formazione = Reading (in) the caselaw: 53 unpublished judgemnts dealing with civil liability law analyzed with annotations and comments by 53 students during their civil law course. The Trento Law and Technology Research Group. Student Paper Series; 25. Trento: Università degli Studi di Trento. ISBN 978-88-8443-626-9

STUDENT PAPER N. 24

La digitalizzazione del prodotto difettoso: stampa 3D e responsabilità civile= The Digital Defective Product: 3D Product and Civil Liability

CAERAN, MIRCO (2016) La digitalizzazione del prodotto difettoso: stampa 3D e responsabilità civile = The Digital Defective Product: 3D Product and Civil Liability. The

Trento Law and Technology Research Group. Student Paper Series; 24. Trento: Università degli Studi di Trento. ISBN 978-88-8443-663-4

STUDENT PAPER N. 23

La gestione della proprietà intellettuale nelle università australiane = Intellectual Property Management in Australian Universities

CHIARUTTINI, MARIA OTTAVIA (2015) La gestione della proprietà intellettuale nelle università australiane = Intellectual Property Management in Australian Universities. The Trento Law and Technology Research Group. Student Paper Series; 23. Trento: Università degli Studi di Trento. ISBN 978-88-8443-626-9

STUDENT PAPER N. 22

Trasferimento tecnologico e realtà locale: vecchie problematiche e nuove prospettive per una collaborazione tra università, industria e territorio = Technology Transfer and Regional Context: Old Problems and New Perspectives for a Sustainable Co-operation among Universitiy, Entrepreneurship and Local Economy

CALGARO, GIOVANNI (2013) Trasferimento tecnologico e realtà locale: vecchie problematiche e nuove prospettive per una collaborazione tra università, industria e territorio. The Trento Law and Technology Research Group. Student Paper Series; 22. Trento: Università degli Studi di Trento. ISBN 978-88-8443-525-5

STUDENT PAPER N. 21

La responsabilità dell'Internet Service Provider per violazione del diritto d'autore: un'analisi comparata = Internet Service Provider liability and copyright infringement: a comparative analysis.

IMPERADORI, ROSSELLA (2014) *La responsabilità dell'Internet Service Provider per violazione del diritto d'autore: un'analisi comparata.* Trento Law and Technology Research Group. Student Paper; 21. Trento: Università degli Studi di Trento. ISBN 978-88-8443-572-9

STUDENT PAPER N. 20

Open innovation e patent: un'analisi comparata = Open innovation and patent: a comparative analysis

PONTI, STEFANIA (2014) *Open innovation e patent: un'analisi comparata.* The Trento Law and Technology Research Group. Student Paper Series; 20. Trento: Università degli Studi di Trento. ISBN 978-88-8443-573-6

STUDENT PAPER N. 19

La responsabilità civile nell'attività sciistica

CAPPA, MARISA (2014) La responsabilità civile nell'attività sciistica = Ski accidents and civil liability. Trento Law and Technology Research Group. Student Paper Series, 19. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 18

Biodiversità agricola e tutela degli agricoltori dall'Hold-Up brevettuale: il caso degli OGM

TEBANO, GIANLUIGI (2014) Biodiversità agricola e tutela degli agricoltori dall'Hold-Up brevettuale: il caso degli OGM = Agricultural Biodiversity and the Protection of Farmers from patent Hold-Up: the case of GMOs. Trento Law and Technology Research Group. Student Paper Series; 18. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 17

Produrre e nutrirsi "bio": analisi comparata del diritto degli alimenti biologici

MAFFEI, STEPHANIE (2013) Produrre e nutrirsi "bio" : analisi comparata del diritto degli alimenti biologici = Producing and Eating "Bio": A Comparative Analisys of the Law of Organic Food. Trento Law and Technology Research Group. Student Paper Series; 17. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 16

La tutela delle indicazioni geografiche nel settore vitivinicolo: un'analisi comparata = The Protection of Geographical Indications in the Wine Sector: A Comparative Analisys

SIMONI, CHIARA (2013) La tutela delle indicazioni geografiche nel settore vitivinicolo: un'analisi comparata. The Trento Law and Technology Research Group. Student Papers Series; 16. Trento: Università degli Studi di Trento. Facoltà di Giurisprudenza.

STUDENT PAPER N. 15

Regole di sicurezza e responsabilità civile nelle attività di mountain biking e downhill montano

SALVADORI, IVAN (2013) Regole di sicurezza e responsabilità civile nelle attività di mountain biking e downhill montano. Trento Law and Technology Research Group. Student Paper; 15. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 14

Plagio, proprietà intellettuale e musica: un'analisi interdisciplinare

VIZZIELLO, VIVIANA (2013) Plagio, proprietà intellettuale e musica: un'analisi interdisciplinare. Trento Law and Technology Research Group. Student Paper; 14. Trento: Università degli Studi di Trento.

STUDENT PAPER N.13

The Intellectual Property and Open Source Approaches to Biological Material

CARVALHO, ALEXANDRA (2013) The Intellectual Property and Open Source Approaches to Biological Material. Trento Law and Technology Research Group. Student Paper Series; 13. Trento: Università degli Studi di Trento.

STUDENT PAPER N.12

Per un'archeologia del diritto alimentare: 54 anni di repertori giurisprudenziali sulla sicurezza e qualità del cibo (1876-1930)

TRESTINI, SILVIA (2012) Per un'archeologia del diritto alimentare: 54 anni di repertori giurisprudenziali sulla sicurezza e qualità del cibo (1876-1930) = For an Archeology of Food Law: 54 Years of Case Law Collections Concerning the Safety and Quality of Food (1876-1930). The Trento Law and Technology Research Group. Student Papers Series, 12.

STUDENT PAPER N.11

Dalle Alpi ai Pirenei: analisi comparata della responsabilità civile per attività turistico-ricreative legate alla montagna nel diritto italiano e spagnolo

PICCIN, CHIARA (2012) Dalle Alpi ai Pirenei: analisi comparata della responsabilità civile per attività turistico-ricreative legate alla montagna nel diritto italiano e spagnolo = From the Alps to the Pyrenees: Comparative Analysis of Civil Liability for Mountain Sport Activities in Italian and Spanish Law. The Trento Law and Technology Research Group. Student Papers Series, 11.

STUDENT PAPER N.10

Copynorms: Norme Sociali e Diritto d'Autore

PERRI, THOMAS (2012) Copynorms: Norme Sociali e Diritto d'Autore = Copynorms: Social Norms and Copyright. Trento Law and Technology Research Group. Students Paper Series, 10.

STUDENT PAPER N. 9

L'export vitivinicolo negli Stati Uniti: regole di settore e prassi contrattuali con particolare riferimento al caso del Prosecco

ALESSANDRA ZUCCATO (2012), L'export vitivinicolo negli Stati Uniti: regole di settore e prassi contrattuali con particolare riferimento al caso del Prosecco = Exporting Wines to the United States: Rules and Contractual Practices with Specific Reference to the Case of Prosecco. Trento: Università degli Studi di Trento (Trento Law and Technology Research Group. Students Paper Series 9)

STUDENT PAPER N.8

Equo compenso e diritto d'autore: un'analisi comparata = Fair Compensation and Author's Rights: a Comparative Analysis.

RUGGERO, BROGI (2011) Equo compenso e diritto d'autore: un'analisi comparata = Fair Compensation and Author's Rights: a Comparative Analysis. Trento: Università degli Studi di Trento (TrentoLawand Technology Research Group. Student Papers Series, 8)

STUDENT PAPER N.7

Evoluzione tecnologica e mutamento del concetto di plagio nella musica

TREVISAN, ANDREA (2012) Evoluzione tecnologica e mutamento del concetto di plagio nella musica = Technological evolution and change of the notion of plagiarism in music Trento: Università degli Studi di Trento (Trento Law and Technology Research Group. Students Paper Series 7)

STUDENT PAPER N.6

Il trasferimento tecnologico università-imprese: profili giuridici ed economici

SIRAGNA, SARA (2011) Il trasferimento tecnologico università-imprese: profili giuridici ed economici = University-Enterprises Technological Transfer: Legal and Economic issues Trento: Università degli Studi di Trento (Trento Law and Technology Research Group. Students Paper Series 6)

STUDENT PAPER N.5

Conciliare la responsabilità medica: il modello "generalista" italiano a confronto col modello "specializzato" francese

GUERRINI, SUSANNA (2011) Conciliare la responsabilità medica: il modello "generalista" italiano a confronto col modello "specializzato" francese = Mediation & Medical Liability: The Italian “General Approach” Compared to the Specialized Model Applied in France. Trento: Università degli Studi di Trento (Trento Law and Technology Research Group. Students Paper Series 5)

STUDENT PAPER N.4

“Gun Control” e Responsabilità Civile: una comparazione fra Stati Uniti e Italia

PODETTI, MASSIMILIANO (2011) “Gun Control” e Responsabilità Civile: una comparazione fra Stati Uniti e Italia = Gun Control and Tort Liability: A Comparison between the U.S. and Italy Trento: Università degli Studi di Trento. (Trento Law and Technology Research Group. Students Paper Series 4)

STUDENT PAPER N.3

Smart Foods e Integratori Alimentari: Profili di Regolamentazione e Responsabilità in una comparazione tra Europa e Stati Uniti

TOGNI, ENRICO (2011) Smart Foods e Integratori Alimentari: Profili di Regolamentazione e Responsabilità in una comparazione tra Europa e Stati Uniti = Smart Foods and Dietary Supplements: Regulatory and Civil Liability Issues in a Comparison between Europe and United States Trento: Università degli Studi di Trento - (Trento Law and Technology Research Group. Students Paper Series; 3)

STUDENT PAPER N.2

Il ruolo della responsabilità civile nella famiglia: una comparazione tra Italia e Francia

SARTOR, MARTA (2010) Il ruolo della responsabilità civile nella famiglia: una comparazione tra Italia e Francia = The Role of Tort Law within the Family: A Comparison between Italy and France Trento: Università degli Studi di Trento - (Trento Law and Technology Research Group. Students Paper Series; 2)

STUDENT PAPER N.1

Tecnologie belliche e danno al proprio combattente: il ruolo della responsabilità civile in una comparazione fra il caso statunitense dell’Agent Orange e il caso italiano dell’uranio impoverito

RIZZETTO, FEDERICO (2010) Tecnologie belliche e danno al proprio combattente: il ruolo della responsabilità civile in una comparazione fra il caso statunitense dell'Agent Orange e il caso italiano dell'uranio impoverito = War Technologies and Home Soldiers Injuries: The Role of Tort Law in a Comparison between the American "Agent Orange" and the Italian "Depleted Uranium" Litigations Trento: Università degli Studi di Trento - (Trento Law and Technology Research Group.