Giorgia Bincoletto

La privacy *by design*

Un'analisi comparata nell'era digitale

Presentazione di
Federico Ferro–Luzzi

Prefazione di
Roberto Caso e Paolo Guarda

Aracne editrice

www.aracneeditrice.it
info@aracneeditrice.it

www.gioacchinoonoratieditore.it
info@gioacchinoonoratieditore.it

via Vittorio Veneto, 20
00020 Canterano (RM)
(06) 45551463

ISBN 978-88-255-2400-0

I edizione: giugno 2019

Indice

Capitolo IV

La privacy *by design* nel diritto europeo

4.1. L'art. 25 del GDPR

Dal 25 maggio 2018 nell'Unione Europea la protezione dei dati personali fin dalla progettazione non è soltanto un *desideratum* o una pratica *recommended*, ma è un obbligo giuridico pienamente esecutivo[1]. Prima di procedere con l'analisi dell'articolo 25 è necessario riferirsi ad affermazioni contenute nella parte iniziale del GDPR.

Nel Regolamento oggetto d'analisi, al Considerando numero 78, si richiede al titolare del trattamento di adottare delle politiche interne e delle misure che soddisfino i principi della protezione dei dati fin dalla progettazione e per impostazione predefinita. Si offrono, tra l'altro, degli esempi concreti di possibili misure implementabili: la riduzione al minimo dell'utilizzo dei dati, la pseudonimizzazione, una maggiore trasparenza sulle funzioni e sullo stesso trattamento, la partecipazione dell'interessato nel controllo dei dati e la possibilità per il titolare di creare e migliorare le caratteristiche della sicurezza[2].

È interessante sottolineare che nello stesso paragrafo si manifesta l'esigenza di incoraggiare i produttori dei servizi, dei prodotti e delle applicazioni, per il cui funzionamento si attua un trattamento di dati personali, a tenere conto del diritto alla

1. Opinion 5/2018 of the European Data Protection Supervisor, *Preliminary Opinion on privacy by design*, 31 May 2018, disponibile in: https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design_en, 3.

2. Cfr. Considerando 78 del Regolamento 2016/679.

loro protezione nelle fasi di sviluppo, di progettazione, di selezione e di utilizzo di questi strumenti, vagliando lo stato dell'arte e così permettendo ai titolari e ai responsabili di adempiere agli obblighi prescritti[3]. Si aggiunge che il principio di PbD e di protezione dei dati *by default*, dovrebbero essere considerati anche per un appalto pubblico; perciò, non solo i privati sono coinvolti, ma anche gli enti statali, aspetto di non poco conto.

Al capo quarto del GDPR, in materia di obblighi generali del titolare e del responsabile del trattamento, si trova l'articolo 25, rubricato "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita"[4]:

> «1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.
> 2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefini-

3. *Ibidem*: «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, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici».

4. Si ricorda che la Rettifica del regolamento (UE) 2016/679 ha specificato che la rubrica deve leggersi «Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita».

> ta, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.
> 3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo»[5].

Il titolare del trattamento, valutate tutte le circostanze descritte dalla norma, deve mettere in atto le misure tecniche e organizzative adeguate ad assicurare una protezione dei dati personali fin dalla progettazione e per impostazione predefinita. La privacy *by design* riguarda l'implementazione di un insieme di garanzie integrate nel sistema e nel processo del trattamento, mentre la privacy *by default* è orientata allo scopo di trattare solo i dati necessari attraverso dei meccanismi predefiniti[6]. L'articolo 25 del GDPR determina un'integrazione *ex lege* delle finalità; così, la tutela dei dati personali diventa parte integrante del loro trattamento[7].

Ora, operando un confronto tra questa norma e il testo dell'articolo 23 dell'iniziale proposta della Commissione, emerge chiaramente che sono stati compiuti dei cambiamenti nel corso dell'elaborazione. In primo luogo, se nel 2012 erano stati forniti solo i criteri dello stato dell'arte e dei costi, qui si hanno molti più elementi da considerare, che sono: la natura dell'ambito di applicazione, del contesto e delle finalità del trattamento dei dati, e i rischi insiti nel trattamento per i diritti e le libertà delle persone fisiche, i quali hanno delle probabilità e gravità diverse tra di loro.

L'aspetto temporale, però, rimane invariato, la data protection privacy *by design* (d'ora in avanti anche DPbD) attraverso le sue misure dovrà essere adottata sia *ex ante*, sia a trattamento pendente.

5. Si è scelto di riportare integralmente l'articolo 25 vista la sua centralità nell'attuale discussione, prendendo a riferimento per praticità la sua versione italiana ricavabile dal sito europeo disponibile in: http://eur-lex.europa.eu/legal-content/IT/TXT/? uri=CELEX %3A32016R0679.

6. G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy. Commentario*, Ipsoa, Milano 2018, 256-257.

7. Ivi, 249.

Secondariamente, le adeguate misure organizzative e procedurali del GDPR, di cui si fornisce l'esempio della pseudonimizzazione, hanno dei fini ulteriori rispetto a ciò che era indicato nel testo della Commissione: esse non sono volte soltanto a garantire la conformità del trattamento alla normativa, ma anche ad attuare efficacemente gli altri principi fondamentali di protezione dei dati, come la minimizzazione, e a tutelare generalmente i diritti degli interessati.

Per quanto riguarda il secondo comma che disciplina la protezione per impostazione predefinita, l'articolo 25 innova il testo precedente quando indica che l'obbligo vale per la quantità delle informazioni raccolte, per il periodo di tempo e altresì per la portata del trattamento e per l'accessibilità dei dati. Poi, il nuovo testo specifica che senza l'intervento della persona fisica i dati personali non devono essere resi accessibili a un numero indefinito di persone fisiche.

Inoltre, rispetto alla proposta, si perdono completamente i due commi 3 e 4 dell'articolo 23, che accordavano maggiori poteri alla Commissione per atti delegati chiarificatori e per la fissazione di standard. La regolamentazione di secondo livello sarebbe stata utile per una maggiore precisazione di contenuto per i titolari, su un piano meno vincolante e più capace di adattarsi all'evoluzione della tecnologia[8].

Allo stesso tempo, però, la scelta evita che gli standard compromettano la neutralità tecnologica delle disposizioni, a vantaggio di una migliore capacità adattiva, di una maggiore flessibilità e di una possibile competitività nelle soluzioni autoimposte dagli operatori[9].

Oggi, residua soltanto un terzo comma che fa riferimento ai meccanismi di certificazione di cui presto si dirà e di cui si tratterà con più ampio respiro nel quinto capitolo del presente lavoro. Questo meccanismo certificatorio potrà essere uno strumento atto a dimostrare la conformità del trattamento ai principi di

8. A. PRINCIPATO, *Verso nuovi approcci alla tutela della privacy: privacy by design e by default settings*, in *Contr. impr. Europa,* 2015, fasc. 1, 215.
9. *Ibid*.

protezione dei dati fin dalla progettazione e per impostazione predefinita. Il passaggio tra le due versioni tiene conto della realizzazione concreta di criteri e strumenti che possano essere davvero utili per le imprese: sarebbe stato più difficile prestare adeguata attenzione ai lavori della Commissione Europea, mentre è sembrato più immediato creare la possibilità di rivolgersi ad enti certificatori esterni per vedersi garantita la compatibilità delle proprie misure con il GDPR e così diminuire il rischio di essere dichiarati responsabili per l'inosservanza degli obblighi di cui all'articolo 25.

A parere di chi scrive, il testo definitivo sulla DPbD ha il pregio di indicare una serie di considerazioni che il titolare del trattamento dovrebbe avere ben presenti una volta che si accinge a definire le misure adottabili nel suo caso concreto; allo stesso tempo è molto ampio, generale e non fornisce molti esempi di pratiche utilmente implementabili, lasciando alla discrezione del titolare e del suo informatico.

Definire e considerare *ex ante* quale sia lo stato dell'arte e i costi di attuazione delle misure non è immediato. Tenere conto della natura, dell'ambito di applicazione, del contesto, delle finalità del trattamento e dei rischi presentabili è molto complesso.

Non si deve dimenticare tuttavia che la scelta di non elencare le tecnologie e le procedure di riferimento è coerente con una tecnica legislativa tecnologicamente neutrale: la norma fissa i principi e le varie linee guida, e sta al progresso della scienza fornire soluzioni sempre più nuove e adeguate allo scopo. Insomma, si apre alle più varie misure tecniche e organizzative, sempreché siano adeguate ed efficaci. Si ricorda, tra l'altro, che nel Considerando numero 78 vengono fornite delle esemplificazioni che possono essere dei punti di partenza per i titolari del trattamento.

Ulteriormente, la neutralità dell'art. 25 è coerente con quanto previsto dall'art. 24 sulla responsabilità del titolare del trattamento: non vengono elencate le misure adeguate "per defini-

zione", ma si lasciano spazi di manovra all'adozione concreta delle stesse[10].

In merito ai criteri di efficacia e di adeguatezza, si sostiene che tali parametri siano strettamente legati al caso concreto ed al suo contesto; perciò, la relativa valutazione sulle misure adottate dovrà essere compiuta da esperti nel settore della privacy, sia giuristi sia tecnici, con competenze in materia di *risk management*[11]. Per poter definire lo stato dell'arte con riferimento all'articolo 25 è stato affermato che questo concetto richiede l'analisi dei più recenti sviluppi tecnologici ed organizzativi associati al trattamento dei dati personali[12]. Il riferimento al costo dell'implementazione non sarebbe limitato alla mera valutazione dei costi e dei benefici, richiedendo, piuttosto, di adottare tra le misure disponibili quelle più adeguate al rischio sotteso al trattamento il cui costo è proporzionato alle risorse di cui dispone il titolare[13].

Si ritiene che lo strumento della certificazione possa offrire un salto di qualità per le società: la DPbD potrebbe essere un elemento di sicurezza e di incentivo per i soggetti commerciali, come dimostrano già ad oggi delle esperienze estere. Ovviamente, i costi della privacy per le imprese potrebbero aumentare di non poco; si può pensare che sarà la futura giurisprudenza europea a dover affrontare il problema dell'approccio di DPbD in relazione ai suoi costi, perché un investimento elevato può essere sintomo di maggior attenzione, ma non è un fattore così determinante.

Si potrebbe ora evidenziare un difetto nell'articolo 25: la norma fa riferimento ai titolari del trattamento, tralasciando chi in concreto opera sulla progettazione, ossia i programmatori, i

10. Cfr, L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il Regolamento privacy europeo, Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, Giuffrè, 2016, 342.

11. L. JASMONTAITE, I. KAMARA, G. ZANFIR-FORTUNA, S. LEUCCI, *Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR*, 4 *EDPL* 168 (2018), 176.

12. Ivi, 178.

13. *Ibid*.

produttori e gli sviluppatori[14]. Ciò potrebbe essere ridimensionato dal fatto che si prevedono delle accortezze che *ex ante* garantiscono la protezione dei dati personali, che si ha l'incentivo per il titolare ad avere dei sistemi informatici conformati alla DPbD, quantomeno per non essere ritenuto responsabile, e che nel GDPR si ha una visione della materia concentrata sulla gestione dell'informazione. Appunto, la disciplina della privacy *by design* sembra focalizzarsi su una corretta e sicura gestione dei dati da parte di chi li detiene[15].

Sull'applicabilità della norma è stato sostenuto, sulla base del Considerando numero 78, che nel GDPR sarebbe presente un onere indiretto di corretta progettazione in capo ai produttori e agli sviluppatori[16]. Infatti, tale Considerando recita 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, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni»[17].

Tuttavia, si tratta di un mero riferimento né restrittivo né vincolante[18]. In aggiunta, il titolare dovrebbe ricorrere ad un responsabile che presti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate affinché il trattamento soddisfi i requisiti del Regolamento[19]. Da questa previsione dell'articolo 28 del GDPR sarebbe possibile dedurre un'indiretta applicazione dell'articolo 25 anche nei confronti della figura del responsabile

14. Anche se c'è chi ha commentato, già a partire dalla proposta di Regolamento, che l'articolo di riflesso si rivolge anche ai produttori di sistemi IT. Si veda B.J. KOOPS, R. LEENES, *Privacy Regulation Cannot Be Hardcoded. A critical comment on the 'privacy by design' provision in data-protection law*, 28 *Int. Rev. Law Comput. Tech.* 1 (2013).

15. Ivi, 217.

16. L.A. BYGRAVE, *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*, 4 *Oslo L. Rev.* 105 (2017), 116.

17. Cfr. Considerando 78 del Regolamento 2016/679.

18. L.A. BYGRAVE, *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*, cit., 118.

19. Cfr. art. 28, co.1 del Regolamento 2016/679.

del trattamento[20]. Su tali questioni, come si vedrà, si è espresso di recente il Garante europeo per la protezione dei dati (*European Data Protection Supervisor*, d'ora in avanti EDPS).

Per quanto riguarda la *data protection by default*, invece, tale obbligo deve essere assolto anteriormente all'avvio del trattamento e ogni volta in cui esso riprenda dopo un'interruzione[21]. Per impostazione predefinita, quindi, devono essere previste delle misure che con automatismo permettano il trattamento dei soli dati personali necessari alla finalità dello stesso. Perciò, la *data protection by default* è un obbligo che potrebbe riflettersi direttamente sui produttori dei beni e servizi[22].

Un'interpretazione dell'articolo 25 è stata effettuata dall'EDPS con l'Opinion numero 5 del 2018 denominata "*Preliminary Opinion on privacy by design*" e pubblicata il 31 maggio 2018[23]. L'EDPS, innanzitutto, distingue tra il principio generale di PbD e l'obbligo previsto dall'articolo 25 definendolo «data protection by design». In questa sede verranno esposte le considerazioni relative a questa seconda accezione[24].

Ebbene, l'autorità descrive le quattro dimensioni della DPbD. In primo luogo, il trattamento dei dati personali, parzialmente o completamente supportato dai sistemi IT, dovrebbe essere sempre il risultato di un *design project*; infatti, l'aspetto progettuale è chiaramente presente nell'articolo 25[25].

La seconda dimensione, invece, riguarda il *risk management approach*: le misure tecniche e organizzative dipendono da chi sono gli interessati e quali sono i loro diritti fondamentali[26]. I

20. L.A. BYGRAVE, *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*, cit., 116. Dello stesso avviso v. L. JASMONTAITE, I. KAMARA, G. ZANFIR-FORTUNA, S. LEUCCI, *Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR*, cit., 173 e 181.

21. F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, cit., 112.

22. Ivi, 114.

23. EDPS, *Opinion n. 5/2018*, cit.

24. Delle considerazioni sul generale principio di privacy *by design* si terrà conto per la successiva l'analisi critica del concetto, dal momento che l'EDPS illustra alcuni aspetti vantaggiosi dell'approccio di PbD e alcune metodologie per la sua adozione.

25. V. EDPS, *Opinion n. 5/2018*, cit., 6.

26. *Ibid.*

criteri di selezione delle misure sono indicati nel primo comma dell'art. 25, ossia la natura, l'ambito di applicazione, il contesto e le finalità del trattamento. Quanto allo stato dell'arte ed ai costi dell'implementazione, si tratta di fattori che possono e devono essere considerati dal titolare; tuttavia, essi devono interpretati in modo da mitigare i rischi in modo adeguato e sufficiente.

Un'altra dimensione della *data protection by design* è la necessità che le misure siano adeguate ed efficaci[27]. In particolare, l'efficacia è strettamente connessa all'obiettivo di garantire i principi applicabili al trattamento dei dati personali[28]. Come verrà indicato nel paragrafo sul concetto di PbD, i principi sono espressamente previsti nell'articolo 5 del GDPR, ma anche altre norme devono essere prese in considerazione[29].

Infine, la quarta dimensione è l'integrazione delle necessarie e interne garanzie nel trattamento dei dati[30]. A differenza di altre garanzie cosiddette "esterne", la DPbD opera all'interno.

Considerando l'insieme delle varie dimensioni, l'EDPS specifica che esse sono parte integrante del principio di *accountability*[31].

Per quanto riguarda la *data protection by default*, l'EDPS ritiene che il secondo comma dell'art. 25 imponga l'adozione di misure tecniche che impediscano il trattamento dei dati per finalità diverse e che prevengano l'accesso pubblico ai dati personali per impostazione predefinita[32]. Ciò risulta, a suo avviso, una particolare espressione dei principi di minimizzazione e limitazione alla conservazione[33].

Malgrado l'articolo 25 non richiami espressamente il responsabile del trattamento, l'EDPS ritiene che la DPbD obblighi indirettamente il titolare a scegliere un responsabile che possa garantirne l'applicazione; perciò, la norma sarebbe impli-

27. *Ibid.*
28. I principi sono espressamente indicati nell'art. 5 del GDPR.
29. V. *infra*, paragrafo 5.
30. Cfr. EDPS, *Opinion n. 5/2018*, cit., 7.
31, *Ibid.* Sull'accountability, v. *infra*, paragrafo 5.
32. Cfr. EDPS, *Opinion n. 5/2018*, cit., 7.
33. V. art. 5, lett. c) e lett. e) del Regolamento 2016/679.

citamente rivolta anche alla figura che tratta i dati personali per conto del titolare[34].

Come già accennato in commento alla norma, l'articolo 25 non fa riferimento ai programmatori, ai produttori e agli sviluppatori. In merito l'EDPS sostiene che il richiamo del Considerando numero 78 al design dei prodotti e dei servizi racchiuda l'obbligo di configurare i sistemi in modo conforme alla normativa in materia di protezione dei dati personali[35]. Ciò nonostante, la stessa autorità ribadisce che tale obbligo non è un obbligo sostanziale del GDPR. È onere del titolare verificare di utilizzare dei prodotti e dei servizi conformi al regolamento perché la responsabilità della violazione dell'art. 25 è a suo carico.

Si badi bene, l'EDPS ha specificato che tale Preliminary Opinion contiene solo gli elementi essenziali per comprendere la portata della norma, ma che delle linee guida dettagliate verranno successivamente pubblicate da essa e dalle altre autorità di controllo[36]. Invero, come si vedrà, il Codice Privacy novellato prevede l'intervento dell'autorità garante per adottare linee guida di indirizzo sulla norma in oggetto[37].

Prescrivendo la necessaria adozione di misure preventive dirette a realizzare il rispetto delle regole ed a ridurre il rischio di pregiudizi, l'articolo 25, dunque, determina una positivizzazione degli obblighi di protezione per l'interessato, scelta legislativa che è stata definita "*opportuna e opportunamente diretta*" a rimarcare l'esigenza di tutela cui è improntata la disciplina del trattamento dei dati personali[38]. La PbD, infatti, è uno strumento operativo previsto per fornire una nuova forma di tutela integrata nel trattamento dei dati e per offrire ai titolari nuove opportunità nella progettazione dei servizi[39].

34. Cfr. EDPS, *Opinion n. 5/2018*, cit., 7.
35. Ivi, 8.
36. Ivi, 3.
37. V. *infra*, paragrafo 4.
38. V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali*, in «Contratto e Impr.», 2018, fasc. 3, 1098.
39. G. D'ACQUISTO, M. NALDI, *Big Data e Privacy by design*, Torino, Giappichelli, 2017, 39.

4.2. Le altre norme del GDPR connesse alla privacy *by design*

Se è evidente che l'articolo 25 ricopre un ruolo centrale per l'oggetto di discussione, è solo proseguendo l'analisi del GDPR che è possibile fornire un quadro completo della nuova DPbD.

Come si affermava nel primo capitolo di questo lavoro, la sicurezza viaggia di pari passo con la privacy.

Tale affermazione è da considerarsi valida anche per il Regolamento n. 2016/679.

All'articolo 30 si richiede al titolare del trattamento e all'eventuale responsabile di tenere un registro delle attività svolte, il quale deve contenere una serie di informazioni, tra le quali, ove possibile, la descrizione generale delle misure di sicurezza tecniche e organizzative assunte ai sensi dell'articolo 32 comma 1[40]. Per l'appunto quest'ultima norma riprende le stesse parole iniziali utilizzate nell'articolo 25 e obbliga il titolare e il responsabile a mettere in atto adeguate misure tecniche e organizzative, affinché si garantisca un livello di sicurezza adatto al rischio.

Le misure richieste dall'articolo 32 sono volte ad assicurare l'applicazione dei principi di integrità e di riservatezza dei dati ai sensi dell'articolo 5 lett. f) del GDPR[41]. Nell'articolo 32 si elencano a tale scopo una serie di misure:

> «a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la di-

40. Cfr. art. 30, co. 1 del Regolamento 2016/679: «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: […] g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1». È necessario specificare in questa sede che, ai sensi del quinto comma dell'articolo 30, dall'obbligo di tenere il registro sono esenti le imprese o le organizzazioni con meno di 250 dipendenti, a meno che non vi sia la possibilità di un rischio per i diritti e per le libertà dell'interessato, o che il trattamento non sia occasionale o che includa delle categorie particolari di dati (di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10).

41. V. EDPS, *Opinion n. 5/2018*, cit., 6.

> sponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento»[42].

Se nell'articolo sulla protezione dei dati fin dalla progettazione non si elencano delle esemplificazioni e, come si è detto, ciò potrebbe essere un vantaggio per l'interpretazione della norma, qui si opera una scelta diversa. Si potrebbe ritenere che, vista la vaghezza dei termini utilizzati, i due articoli debbano sempre essere letti congiuntamente: il titolare mette in atto le misure tecniche e organizzative per rispettare il principio di DPbD e allo stesso tempo garantire la sicurezza del trattamento.

Da entrambe le norme emerge chiaramente l'importanza della valutazione del rischio, che in relazione alla sicurezza dovrà vagliare la possibilità di distruzione, di perdita, di modifica, di divulgazione non autorizzata o di accesso ai dati, in modo accidentale o illegale, in relazione ai dati personali trasmessi, conservati o comunque trattati[43].

Poi, anche nell'articolo 32, si statuisce che l'adesione ad un meccanismo di certificazione potrebbe essere utilizzata per dimostrare la conformità con il GDPR. In aggiunta, si prevede la stessa possibilità anche per l'adozione di un codice di condotta approvato ai sensi dell'articolo 40[44].

La presenza di questi codici è volta a contribuire alla corretta applicazione del GDPR ed è compito degli Stati Membri, delle autorità di controllo, del comitato previsto all'interno del Regolamento e della Commissione incoraggiarne l'elaborazione, con l'attenzione nei confronti delle specificità dei settori del trattamento e delle esigenze delle varie tipologie di imprese[45]. I soggetti che possono elaborare i codici di condotta, modificarli o prorogarli sono le associazioni e gli altri organismi rappresen-

42. Cfr. art. 32, co. 1, del Regolamento 2016/679.
43. Cfr. art. 32, co. 2, del Regolamento 2016/679.
44, Cfr. art. 32, co. 3, del Regolamento 2016/679.
45. Cfr. art. 40, co. 1, del Regolamento 2016/679.

tanti le categorie di titolari del trattamento, al fine di precisare cosa significhi in termini concreti applicare le nuove norme[46]. Al secondo comma dell'articolo appena citato vengono elencate, a titolo di esempio, una serie di norme del GDPR che potrebbero essere meglio esplicate grazie all'adozione dei codici di condotta e tra queste sono comprese le misure e le procedure di cui agli articoli 24, 25, 32, che contengono anche la disciplina della *data protection by design* e *data protection by default*[47].

I codici di condotta, e le loro successive modifiche o proroghe, sono elaborati dalle associazioni e dagli altri organismi, ma devono essere vagliati dalle autorità di controllo, attraverso un parere di conformità al Regolamento e, se approvati, sono da queste registrati e pubblicati[48].

Il GDPR inserisce non solo i codici come strumenti per garantirne l'adeguata implementazione, ma anche la certificazione. Ai sensi dell'articolo 42 si incoraggia, particolarmente al livello dell'Unione Europea, l'istituzione di meccanismi di certificazione della protezione dei dati, di sigilli e di marchi[49]. La certificazione è volontaria, non riduce la responsabilità dei soggetti ed è rilasciata da organismi accreditati presso le autorità di controllo o l'organismo nazionale di accreditamento. A differenza dei codici di condotta, che sono finalizzati a definire modalità particolari di applicazione del GDPR in specifici settori, la certificazione riguarda qualsiasi trattamento e si limita ad attestarne la conformità[50]. Analizzando il rapporto tra ente certificatore e titolare del trattamento in Italia, è stato affermato che tra tali soggetti viene sottoscritto un contratto atipico, di durata

46. Cfr. art. 40, co. 2, del Regolamento 2016/679.

47. Cfr. art. 40, co. 2, lett. h), del Regolamento 2016/679.

48. Cfr. art. 40, co. 5, del Regolamento 2016/679: «L'autorità di controllo esprime un parere sulla conformità al presente regolamento del progetto di codice, della modifica o della proroga e approva tale progetto, modifica o proroga, se ritiene che offra in misura sufficiente garanzie adeguate. 6. Qualora il progetto di codice, la modifica o la proroga siano approvati ai sensi dell'articolo 55, e se il codice di condotta in questione non si riferisce alle attività di trattamento in vari Stati membri, l'autorità di controllo registra e pubblica il codice».

49. Cfr. art. 42, co. 1, del Regolamento 2016/679.

50. F. PIZZETTI (a cura di), *Intelligenza artificiale,* cit., 157.

ed a effetti obbligatori[51]. Come si vedrà nel quinto capitolo del presente lavoro non mancano all'estero delle esperienze certificatorie già in atto sulla PbD.

Un richiamo alle misure tecniche e organizzative è presente nell'articolo 34 del GDPR sulla comunicazione di una violazione dei dati personali all'interessato[52]. In particolare, qualora il titolare del trattamento abbia messo in atto delle misure adeguate di protezione sui dati oggetto di violazione e destinate a rendere tali dati intellegibili, la comunicazione all'interessato non è richiesta[53].

Se tutto questo apparato di garanzie non fosse sufficiente e il trattamento dei dati non fosse conforme al regolamento, le autorità di controllo infliggeranno delle sanzioni amministrative pecuniarie, come previsto dall'articolo 83 del GDPR. Quando un'autorità deve agire in questo senso, sia nel momento della decisione sull'imposizione, sia in quello della fissazione dell'ammontare della somma dovuta, essa dovrà tenere in debito conto vari criteri, tra i quali il grado di responsabilità del titolare del trattamento o del responsabile con riferimento alle misure tecniche e organizzative degli articoli 25 e 32[54]. Gli obblighi contenuti in queste norme, se non assolti, possono portare all'imposizione di sanzioni amministrative pecuniarie fino a dieci milioni di euro o per le imprese fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore[55].

51. A.R. POPOLI, *Codici di condotta e certificazioni*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy*, cit., 415.

52. Cfr. art. 34 del Regolamento 2016/679.

53. Cfr. art. 34, comma 3, lett. a), del Regolamento 2016/679. Sulla comunicazione di *data breach* sono state pubblicate a Novembre 2018 le *Guidelines on personal data breach notification for the European Union Institutions and Bodies* da parte dell'EDPS.

54. Cfr. art. 83, co. 2, lett. d), del Regolamento 2016/679: «d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32».

55. Cfr. art. 83, co. 4, del Regolamento 2016/679: «4. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10.000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore: a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43».

Insomma, ciò che si può affermare è che per il GDPR la DPbD è un obbligo giuridico soggetto alla valutazione della probabilità dei rischi per le violazioni dei diritti e delle libertà. Le aziende, come si è ripetuto più volte, devono cercare di adottare le misure già quando progettano le modalità e le politiche del trattamento dei dati che raccolgono, valutando il rischio per gli utenti in relazione alle attività. Questa valutazione è un aspetto caratteristico del Regolamento 2016/679, visto che si prevede all'articolo 35 il Data Protection Impact Assessment (DPIA). Quando il trattamento prevede l'uso di nuove tecnologie, considerati la sua natura, l'oggetto, il contesto e la finalità, e può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, si dovrà effettuare una valutazione di impatto sulla protezione dei dati[56]. I rischi per la privacy, infatti, hanno diversi gradi di probabilità e gravità. Si tratta di un meccanismo erede di quel documento programmatico sulla sicurezza che si è presentato nel primo capitolo di questo lavoro.

Inoltre, come precisato dal Gruppo articolo 29 nelle "*Guidelines on Data Protection Impact Assessment (DPIA)*" la valutazione di impatto, da eseguirsi prima dell'inizio del trattamento, è uno strumento per assicurare la DPbD[57]. La DPIA si sposa con l'approccio di DPbD perché l'analisi dei rischi è l'antecedente logico alla mitigazione degli stessi attraverso l'adozione di soluzioni progettuali per la tutela dei dati personali[58]. Una corretta applicazione della DPbD potrebbe rendere superflua una valutazione finale dei rischi perché il rischio è prevenuto dall'iniziale modellazione del prodotto o del servizio[59].

56. Cfr. art. 35, co. 1, del Regolamento 2016/679.

57. ART 29 WORKING PARTY, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, adopted on 4 April 2017, WP 248 rev.01, 14.

58. A. MANTELERO, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. valutazione d'impatto e consultazione preventiva (artt. 32-39)*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy*, cit. 308.

59. *Ibid.* Per una più completa descrizione della valutazione dei rischi e delle norme del GDPR ad essa dedicate, si veda l'intero capitolo del predetto volume alle pp. 289-330; si veda anche F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, cit., 63-73.

La soluzione di DPbD sarà ricercata nel caso concreto: ogni categoria di trattamento, ogni singolo trattamento, sarà circondato da limiti e garanzie suoi propri e collegati al rischio percepito, ma saranno tutti presenti fin dalla sua progettazione. Il tempo e la tecnologia sono due variabili sempre in movimento e giocheranno sempre un ruolo chiave per i titolari del trattamento dei dati personali.

A livello giuridico la normativa sarà più flessibile, non rischierà di diventare obsoleta a causa del costante progresso tecnologico e i dati personali saranno protetti con maggiore sicurezza ed efficacia, perché si avrà una protezione *ex ante* più adeguata e funzionale. È vero che i costi sono molto alti per le aziende e che sarà più difficile dimostrare la presenza di responsabilità perché la prova richiede alle autorità delle valutazioni molto più complesse, con il rischio che siano eccessivamente discrezionali. Dovendosi considerare l'organizzazione e l'allocazione delle risorse per la protezione della privacy, le piccole e le grandi aziende potrebbero soggiacere ad un trattamento differente.

Allo stesso tempo, la privacy assume grazie al GDPR un ruolo ancora più significativo e un'importanza vitale per i soggetti economici; infatti non c'è più la possibilità di eludere in qualche modo il sistema predisponendo soltanto vari regolamenti interni all'azienda, perché le misure rispettose della DPbD e della *data protection by default* sono vincolanti e soggette ad un pesante rischio sanzionatorio.

In conclusione, si possono riportare alcune delle parole del discorso di Viviane Reding, membro della Commissione Europea responsabile per *l'information society* e i media, tenutosi a Bruxelles di fronte al Parlamento Europeo nell'occasione del *Data Protection Day* il 28 gennaio del 2010:

> «Here we need a change of approach: Businesses must use their power of innovation to improve the protection of privacy and personal data from the very beginning of the development cycle. Privacy by Design is a principle that is in the interest of both citizens and businesses. Privacy by Design will lead to better protection for individuals, as well as to trust and confidence in new services and products that will in turn

> have a positive impact on the economy. I have seen some encouraging examples, but much more needs to be done»[60].

La PbD rappresenta un cambiamento di approccio, lo si è ampiamente dimostrato; è un principio che avvantaggia gli individui e allo stesso tempo potrebbe creare dei benefici ai soggetti commerciali. Si è detto come sia stato esplicitato solo mercé della nuova normativa europea in materia di protezione dei dati; eppure, analizzando la legislazione precedente, sia italiana, sia sovranazionale, tanto cogente, quanto di *soft law*, potrebbero essere rilevate delle sue tracce precedenti, che ne dimostrano la bontà e la non così totale novità.

4.3. Prima del GDPR: alla ricerca della privacy *by design* nella normativa europea ed italiana e nei documenti di *soft law*

È certamente vero che la PbD ha trovato la sua finale codificazione nel GDPR; compiendo un'analisi storica e interpretativa, si possono, però, rilevare delle tracce di questo principio già in precedenti norme europee ed italiane e in documentazioni di *soft law* provenienti dalle autorità garanti della privacy o dalla Commissione Europea.

In questo paragrafo si intende dare evidenza a questo percorso, che si è rivelato un passo fondamentale per comprendere che il contenuto della stesura finale dell'articolo 25 del Regolamento 2016/579 si è formato sì tramite i lavori redazionali degli organi europei, ma anche grazie alla presenza nel contesto di norme e di riflessioni nel corso degli ultimi anni.

Iniziando con la 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 (*Data Protection Directi-*

60. Il testo del discorso è rinvenibile nel sito: http://europa.eu/rapid/press-release_SPEECH-10-16it.htm.