UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI FILOSOFIA, SOCIOLOGIA, PEDAGOGIA E PSICOLOGIA APPLICATA

DIPARTIMENTO DI SCIENZE POLITICHE, GIURIDICHE E STUDI INTERNAZIONALI

CORSO DI LAUREA IN COMUNICAZIONE

Accountability e *Data Protection Officer*: elementi di un nuovo paradigma nel GDPR

Relatore:
Ch.mo Prof. Vincenzo Durante

Laureando:
Filippo Lorenzelli
Matricola n. 1223607

ANNO ACCADEMICO 2021 - 2022

“Suppongo che il resto di voi stia aspettando che io vomiti alcune profonde parole di saggezza […].
Sentite: il mondo ha bisogno di persone come voi, il mondo letteralmente brama e vi aspetta. Abbracciate questa responsabilità e cavalcatela: andate là fuori, guadagnatevi da vivere e restituite agli altri. Non sarà facile, non lo sarà mai, il più delle volte vi ritroverete da soli, ma dovrete continuare a tenere duro.
Io vi supplico, non arrendetevi mai alla mediocrità, come il 98 percento del mondo, perché è certo che farete a voi stessi, e al mondo, un grave torto.
Non lasciate che la vostra intelligenza vada sprecata … e avete una sola occasione per farlo, una sola […] occasione. Non lasciate che vi sfugga neanche un momento: afferratelo, portatelo a voi e fatelo vostro. Festeggiate ogni momento, perché ogni […] respiro va festeggiato.
Ricordate: la vita è un canto d’uccello.”

Dal film *Arrivederci Professore* di Wayne Roberts, 2018.

A chi c’è stato nel mio momento più buio. Questa è la mia favola, ma è scritta sulle vostre pagine.

Indice

Introduzione

Il tema della protezione dei dati personali è forse uno dei più dibattuti al giorno d'oggi, se non altro per la frequenza con cui pervade le nostre attività quotidiane. Nonostante ciò, quella che viene frettolosamente chiamata *privacy*[1] ha assunto agli occhi dei titolari (chi utilizza i dati personali altrui) a volte i tratti di un aggravio burocratico, mentre gli interessati (ovvero chi cede i propri dati personali, cioè tutti) la considerano spesso un insieme di fastidiosi *banner* che precludono l'accesso a tutti i siti internet[2].

Con una simile considerazione generale può sembrare quantomeno strano che gli organi governativi nazionali e sovranazionali dedichino al tema della *data protection* lunghe discussioni con una certa regolarità. Inoltre, il legislatore europeo ha emanato, nel corso degli anni, una lunga serie di norme riguardanti le informazioni personali, la più importante delle quali è sicuramente il Regolamento europeo n. 679 del 2016, noto a tutti come GDPR (*General Data Protection Regulation*).

Questa dissonanza tra l'attività normativa dei legislatori e le opinioni che costituiscono la coscienza comune può sembrare strana, soprattutto a chi ha letto Durkheim[3]; ecco perché in questo lavoro abbiamo voluto cominciare indagando sui primi passi della tutela di dati personale, cercando di capirne le radici ideologiche e sociali.

Proprio per questo motivo siamo partiti da un altro diritto che oggi riteniamo fondamentale (tutelato indirettamente dalla Costituzione[4]) che possiamo considerare l'antenato della *data protection*, ovvero il diritto alla riservatezza, la cui discussione inizia negli Stati Uniti con la pubblicazione di un saggio di due avvocati di Boston, Louis Brandeis e Samuel Warren, nel 1890[5], in risposta alla diffusione di una nuova tecnologia: la fotografia.

---

[1] Tratteremo il dualismo privacy e *data protection* nel cap. 1, § 1.1.3.

[2] Cfr. PIZZETTI F., *Relazione Garante Privacy 2005*, presentata alle Camere il 7 luglio 2006, Doc-Web 1303712, in https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1303712 e BERNARDI N. & AL., *Privacy officer, la figura chiave della data protection europea. Manuale operativo*, Milanofiori Assago (MI), Ipsoa, 2013, pp. 2 s.

[3] Il sociologo Émile Durkheim (1858 – 1917) ha analizzato il rapporto tra la coscienza comune di un popolo e le leggi di cui questo si è dotato. V. SANTAMBROGIO A., *Introduzione alla sociologia. Le teorie, i concetti, gli autori*, Roma, Laterza, 2008, pp. 66 - 78.

[4] V. *infra*, cap. 1, § 1.1.2.

[5] V. nota n. 3, p. 1.

Questo rapporto tra l'evoluzione dei diritti più genericamente riferibili al tema della *privacy* e il progresso tecnologico è un altro degli aspetti su cui si è sviluppata l'indagine nel presente lavoro.

Appartenendo però noi al vecchio continente, abbiamo volto lo sguardo alla discussione sulla tutela della vita privata nel panorama europeo che, questa volta sicuramente in linea con Durkheim, è stata influenzata dal retaggio storico dei totalitarismi, poco dopo la fine dei quali si è sviluppata.

Con l'avvento delle organizzazioni sovranazionali, l'insieme dei *corpus* normativi riguardanti riservatezza e *data protection* ha raggiunto dimensioni importanti; in particolare, questo secondo filone ha trovato una tappa fondamentale nella Direttiva europea n. 46 del 1995.

Tale atto normativo, che ha assunto tra gli addetti ai lavori il nome di "Direttiva madre", è rimasto in vigore per circa vent'anni, periodo nel quale ha evidenziato però alcune lacune, soprattutto a livello di efficienza reale e onerosità per i titolari.

Proprio per questi motivi, congiuntamente alla continua evoluzione degli strumenti che permettono l'analisi dei dati, l'Unione Europea ha negli ultimi anni sviluppato un nuovo quadro normativo avente come protagonista il già citato GDPR, per mezzo del quale ha avviato una rivoluzione del modo in cui è implementata la *data protection.*

Nel presente lavoro ci siamo quindi concentrati su due elementi che possono essere ritenuti centrali in questa rivoluzione: il principio di *accountability*[6] e la figura professionale del *Data Protection Officer*.

In concreto, il principio di *accountability*, che si è tradotto in uno spostamento del focus e della tipologia delle prescrizioni dell'atto normativo[7], sostituisce le numerose prescrizioni della Direttiva 94/46/CE (e delle norme che ne sono derivate) con una serie di principi[8] ai quali il titolare deve conformare i propri trattamenti, scegliendo però egli stesso, con grande autonomia, le misure specifiche da adottare di volta in volta[9]. Nello specifico l'*accountability* si configura in un meccanismo a due livelli, il primo dei quali è composto da alcune soluzioni minime che il titolare deve adottare per rispettare il Regolamento, mentre il secondo si articola in una serie di misure aggiuntive che il titolare può decidere volontariamente di adottare, garantendo così una

[6] V. *infra*, cap. 2, § 2.1.

[7] V. *infra*, cap. 1, § 1.2.2 a confronto con cap. 2, § 2.1.

[8] I principi sono contenuti nell'art. 5 del Regolamento 2016/679/UE.

[9] V. *infra*, cap. 2, § 2.1.

maggiore tutela dei dati personali[10].

Inoltre, il principio di *accountability* prevede che il titolare debba tenere traccia di tutte le decisioni e le valutazioni concernenti ciò che abbiamo appena descritto, essendo di conseguenza in grado di dimostrare la propria conformità alla normativa in caso di controllo da parte dell'autorità preposta, il cui intervento avviene solo in un momento successivo alla messa in atto dei trattamenti[11].

L'introduzione del principio di *accountability* accresce quindi la centralità delle *data protection* all'interno di tutte le organizzazioni che trattano informazioni personali; il fine ultimo di questo spostamento è la creazione di una vera e propria cultura della protezione dei dati anche a livello micro[12].

A tale scopo, il GDPR ha introdotto la nuova figura professionale del *Data Protection Officer*[13] che, interno alle aziende, ibrida in sé le funzioni di consulenza e di controllo del rispetto delle norme, con tutte le contraddizioni che ne derivano.

Egli deve cioè porsi sia come primo supporto nella messa in atto dei trattamenti e nella gestione degli stessi in conformità alle normative vigenti, ma anche come primo controllore del rispetto di quest'ultime. La molteplicità e l'eterogeneità dei compiti assegnati al *Data Protection Officer*[14] hanno suscitato le perplessità di una parte della dottrina[15] e hanno esposto i soggetti che ricoprono il ruolo a situazioni di conflitto di interessi, alcune delle quali sono state sanzionate dalle Autorità di controllo[16].

Ad ogni modo, l'introduzione del principio di *accountability* e della figura del *Data Protection Officer* rappresenta il tentativo da parte del legislatore europeo di superare la storica dicotomia tra regolazione e regolato, tra controllore e controllato, cercando di ripristinare quello scollamento tra le leggi e la coscienza collettiva cui abbiamo accennato in apertura.

---

[10] V. *infra*, cap. 2, § 2.1.3.

[11] *Ibidem*.

[12] Cfr. RICCIO, G. M., SCORZA, G., & BELISARIO, E., *GDPR e normativa privacy. Commentario*, Milano, Wolters Kluwer, 2018, p. 237.

[13] V. *infra*, cap. 3, § 3.2.

[14] V. art. 39, Regolamento 2016/679/UE.

[15] V. *infra*, cap. 3, § 3.2.3.

[16] V. *infra*, cap. 3, § 3.2.4.

Capitolo 1: La privacy prima del Regolamento

1.1 Origini della tutela della riservatezza

Sebbene il diritto alla riservatezza e il diritto alla protezione dei dati personali siano due principi molto diversi tra loro, è innegabile che il secondo affondi le sue radici nel processo di definizione del primo[1].

La storia della tutela della riservatezza va di pari passo con l'invenzione di quelle tecnologiche che, per loro stessa natura, ne hanno rappresentato una minaccia. Infatti, prima che J. N. Niépce trovasse il modo di utilizzare la luce per imprimere una parte di realtà su una pellicola, quasi nessuno aveva mai ritenuto necessario avviare un dibattito sulla tutela di una parte della propria vita[2].

Così è proprio in risposta al crescente perfezionamento della fotografia che Louis Brandeis e Samuel Warren stilano, nel 1890, l'articolo generalmente considerato il capostipite della tutela della riservatezza: *The Right to be let alone*[3], comunemente tradotto nella nostra lingua come "il diritto di essere lasciati soli"[4], oppure, preferibilmente, "il diritto di essere lasciati in pace"[5]. Da quel momento si apre il grande dibattito che porta

---

[1] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, G. Giappichelli, 2016, p. 43.

[2] Cfr. *ivi,* pp. 7, 47. Ovviamente si possono trovare degli accenni al tema della riservatezza anche in epoche precedenti, nelle quali non trovavano posto quelle idee e quei su cui si fondano gli stati moderni. Lo stesso Pizzetti ha definito la riservatezza come la progenie di "*un tema vecchio come il mondo, legato alla necessità di proteggersi dalla curiosità degli altri e dal controllo asfissiante del potere"* (*ivi*, p. 14). E ancora "*Il desiderio, se non il diritto, alla 'privacy', è sempre esistito a memoria d'uomo ed è sempre stato declinato sotto due diversi aspetti, uno dei quali, quello più antico, è legato alla stessa concezione che è alla base del diritto di proprietà.*" (*ivi*, p. 23). Ad ogni modo, Pizzetti colloca, nello stesso volume, l'inizio della discussione del tema a partire dal 1890 (*ivi*, pp. 43 s.).

[3] V. BRANDEIS L. & WARREN S., *The right to privacy*, in *Harvard Law Review*, vol 4 n. 5, 15/12/1890, pp 193 – 220, in https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf.

[4] Lo stesso Pizzetti, in *Privacy e diritto europeo*, cit., propende per questa traduzione, ad esempio, riguardo al diritto in generale, a p. 24.

[5] A preferire questa traduzione è, ad esempio, ATELLI M., *Il diritto alla tranquillità individuale*, Napoli, Jovene, 2001, pp. 1, 7 ss.: "*Sino ad un non lontano passato, com'è noto, la formula linguistica "diritto di essere lasciati soli" è stata intesa nella letteratura giuridica come evocativa essenzialmente di un diritto alla privacy concepito secondo l'idea originaria di strumento di protezione di fronte all'altrui curiosità, ovvero «contro» l'altrui interesse a conoscere.* (p.1); "*Potere, questo, che sembra appropriatamente condensabile, per la verità, in una formula diversa dal tradizionale "diritto di essere lasciati soli", anche perché, come ha sottolineato attenta dottrina, la traduzione idiomatica dell'espressione anglosassone "right to be let alone" corrisponde in lingua italiana al "diritto di essere lasciati in pace", che di certo meglio esprime l'ampiezza effettiva dell'interesse all'intimità e alla vita privata.*" (pp. 7 s.).
Si veda, inoltre, ZATTI P. & COLUSSI V., *Lineamenti di diritto privato*, Padova, Cedam, VIII ed., 2001, p. 158: "*Si fa riferimento alla difesa di una zona di intimità, in cui «essere lasciati in pace» (right to be let alone): il diritto si configura qui come un potere di regolare l'accesso alla propria sfera di intimità, di permettere o vietare l'intromissione di chi vuole conoscere ciò che più da vicino ci concerne…*".
In sostanza, il soggetto del *Right to be let alone* ha il potere di decidere, non solo a chi permettere di entrare nella propria sfera privata, ma anche con chi condividere informazioni che lo riguardano. Questa duplice funzione non è

alla tutela della riservatezza prima e, anche in seguito alla diffusione di nuove tecnologie, alla tutela dei dati personali poi.

Se i natali della riservatezza moderna vengono collocati, anche da studiosi europei[6], negli Stati Uniti, da qui in avanti la concezione della riservatezza in Europa e nel Nuovo Mondo seguiranno strade diverse. D'altronde l'Europa è un insieme di Stati eterogenei che, fino alla metà del secolo scorso, erano in forte tensione fra loro; inoltre, alcune di queste nazioni, dopo essersi faticosamente liberate delle monarchie assolute, hanno adottato quasi subito regimi totalitari[7]. È proprio il termine "totalitario" ad avere grande importanza in questa fase: uno Stato totalitario è un'istituzione che permea ogni frangente della vita dei propri cittadini, che plasma ogni dettaglio e che quindi, non lascia spazi alla riservatezza del singolo[8]. Con un tale retaggio storico, è naturale che quando, dopo la fine delle guerre, si sviluppano i diritti fondamentali delle persone, si ritiene che la vita privata dei singoli vada difesa prima di tutto *contra Imperium*: ovvero come una di quelle che oggi chiamiamo libertà negative[9].

In America il problema della riservatezza è invece, almeno nelle prime fasi della sua evoluzione, legato principalmente ai media: infatti, Brandeis e Warren introducono la discussione partendo dal tema di quando la stampa abbia il diritto di diffondere informazioni relative a una persona[10]. Vi era quindi la necessità di determinare il rapporto tra due diritti: quello di cronaca (e dall'altro lato il diritto dei cittadini ad essere informati) e quello del singolo alla protezione della propria vita privata[11] e "*della libertà di agire in tale ambito senza controlli e senza dover temere che la conoscenza delle sue azioni possa essere legittimamente diffusa*"[12].

---

sufficientemente manifesta nella traduzione "diritto di essere lasciati soli", che sembra proiettare ad un "*indifferenziato e approssimativo interesse all'isolamento*", ATELLI M., *Il diritto alla tranquillità individuale*, cit., p. 9.

[6] V., ad esempio, PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali*, pp. 8, 47 e FINOCCHIARO G., *Inquadramento teorico*, in FINOCCHIARO G. (a cura di), *Privacy e protezione dei dati personali: disciplina e strumenti operativi*, Torino, Zanichelli editore, 2016 (I ed. 2012), p. 8.

[7] V. PIZZETTI F., *Privacy e il diritto europeo*, cit., p. 52 s.

[8] Cfr. GOFFMAN E., *Istituzioni totali (Eng. Asylums)*, Torino, Einaudi, 2003.

[9] Cfr. MANTELERO A. *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati,* in *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali,* in FINOCCHIARO G. (a cura di), Torino, Zanichelli, 2017, pp. 289 s.

[10] V. PIZZETTI F., *Privacy e il diritto europeo*, cit., pp. 44 s.

[11] *Ibidem.*

[12] *Ivi,* p. 44.

1.1.1 Prime regolamentazioni della tutela della riservatezza in Europa

In Europa, tra il 1947 e il 1950 vengono emanate due norme fondamentali per lo sviluppo del tema. La prima è la Costituzione italiana ed in particolare l'art. 2[13]; la seconda è la Convenzione europea dei diritti dell'uomo, approvata nel 1950 a Strasburgo[14], il cui art. 8[15] è rubricato "*Diritto al rispetto della vita privata e familiare*". La Convenzione è il primo testo normativo in Europa che disciplina *esplicitamente*[16] la riservatezza. Qui notiamo che la *ratio* dell'art. 8 è quella di tutelare la riservatezza anche *dallo Stato*: il secondo comma limita infatti l'"*ingerenza di un'autorità pubblica*", mentre il primo cita la "*corrispondenza*" tra le sue tutele[17]. Non vi è invece cenno al rapporto tra riservatezza e libertà di manifestazione del pensiero, elemento fondante, invece, del *Right to privacy* di Brandeis e Warren[18]. Inoltre, l'ingerenza dello Stato viene ritenuta come lecita solo in alcune eccezioni, che devono trovare fondamento nella tutela della "*società democratica*". Questo esclude ogni forma di controllo generalizzato sui cittadini, sia per le loro attività, sia per le informazioni che li riguardano e pone quindi le premesse per un più specifico diritto alla protezione dei dati personali[19].

1.1.2 In Italia: il mutamento interpretativo della Costituzione

In Italia, nonostante la ratifica della CEDU avvenuta nel 1955, la giurisprudenza non ritenne inizialmente di riconoscere un generale diritto alla riservatezza nel nostro ordinamento. La Cassazione, infatti, nel famoso

---

[13] "*La repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale*". Evidentemente, questo articolo non tratta in modo esplicito il tema della riservatezza, ma sarà comunque molto importante per l'evoluzione di questa tutela in Italia (v. *infra*, § 1.1.2).

[14] Il nome completo è *Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali* (CEDU), adottata nel 1950 dal Consiglio d'Europa; essa rappresenta il testo fondamentale europeo in materia di diritti dell'uomo. La Convenzione è stata ratificata dall'Italia con la l. 4 agosto 1955, n. 848. È doveroso ricordare che aderiscono alla convenzione anche nazioni non facenti parte dell'Unione Europea, come Russia e Turchia.

[15] *"1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui."* Art. 8, *Convenzione per la salvaguardia dei diritti dell'Uomo e delle Libertà Fondamentali,* Consiglio d'Europa, Strasburgo, 1950 – per questo testo è stato utilizzato il più recente documento ufficiale, in https://www.echr.coe.int/documents/convention_ita.pdf.

[16] Si faccia attenzione a questo avverbio perché, come per quanto detto sull'art. 2 Cost. (v. *infra*, § 1.1.2).

[17] Tendenzialmente chi ha la capacità di limitare la segretezza delle corrispondenze private è lo Stato. Questo elemento accentua la *ratio contra Imperium* di questo articolo (v. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali*, cit., p. 58, nota n. 3).

[18] V. PIZZETTI F., *Privacy e il diritto europeo*, cit., p. 58.

[19] *Ibidem*.

caso "Caruso" del 1956, statuì che "*nessuna disposizione di legge autorizza a ritenere che sia stato sancito, come principio generale, il rispetto assoluto alla intimità della vita privata e tanto meno come limite alla libertà dell'arte*"[20]. Il caso riguardava una serie di riprese girate nell'abitazione privata del noto cantante lirico: anche qui si può notare come la discussione sulla tutela della vita privata si intrecci con l'evoluzione dei mezzi tecnologici, in particolare quelli in grado di lederla[21].

Era, come ovvio, un'Italia diversa dalla nostra in moltissimi aspetti: non vi era ancora un'adeguata sensibilità sul tema della riservatezza e, soprattutto, l'art. 2 Cost. veniva interpretato in modo "chiuso", ovvero ritenendo che "*i diritti inviolabili dell'uomo*" in esso menzionati si limitassero ai soli diritti citati negli articoli successivi[22].

A partire dagli anni '70, questa linea interpretativa lasciò spazio a quella secondo cui l'art. 2 Cost. andava visto come una "fattispecie aperta". Ciò permise di considerare tutelati dall'art. 2 anche nuovi diritti, non necessariamente esplicitati nella Costituzione, ma che, con l'evolversi della società, erano diventati, secondo la coscienza comune, parte integrante della personalità del singolo[23]. Uno di questi fu appunto quello della tutela della riservatezza.

Infatti, fu proprio la Corte costituzionale a riconoscere esplicitamente per la prima volta il diritto alla riservatezza, nella sentenza n. 38 del 1973: "*Non contrastano con le norme costituzionali ed anzi mirano a tutelare e a realizzare i fini dell'art. 2 affermati anche negli artt. 3, secondo comma, e 13, primo comma, che riconoscono e garantiscono i diritti inviolabili dell'uomo, fra i quali rientra quello del proprio decoro, del proprio onore, della propria rispettabilità, riservatezza, intimità e reputazione, sanciti espressamente negli artt. 8 e 10 della Convenzione europea sui diritti dell'uomo*"[24]. Il cambiamento è fondamentale, perché con questa nuova interpretazione estensiva il diritto alla riservatezza trova un fondamento normativo nella Carta

---

[20] Cass. civ. sent. 22 dicembre 1956, n 4487 in *Il Foro Italiano*, 1957, vol. 80, I, cc. 4 - 11. Lo stesso principio viene poi ripetuto anche in Cass. civ. sent. 7 dicembre 1960, n. 3199, in *Il Foro Italiano*, 1961, vol 84, I, cc. 43/44 - 47/48.

[21] V. nota n. 2, p. 1.

[22] Cfr. DE MARTINI C., *Il diritto all'identità personale nell'esperienza operativa*, in AA.VV., *La lesione dell'identità personale e il danno non patrimoniale*, Milano, 1985, pp. 94 s.

[23] *Ibidem.*

[24] Corte cost., sentenza 12 aprile 1973, n. 38, in www.cortecostituzionale.it e in https://www.foroplus.it/visualizza.php?pag=1&ndoc=1630187G&sha1=7a2ed966edd4c4948fef8aff61cadbfacce16391&ur=MTAzNjU2Mg==.

fondamentale dell'ordinamento.

Un'autorevole, seppur minoritaria, dottrina aveva invece ritenuto di rinvenire il fondamento costituzionale della segretezza della vita privata nella libertà di espressione, tutelata dall'art. 21 Cost. Secondo tale orientamento, dal momento che il diritto a manifestare il proprio pensiero contiene anche la libertà negativa di astenersi dal manifestarlo, su tale astensione si baserebbe anche la tutela costituzionale della segretezza della vita privata, in quanto diritto della personalità[25].

1.1.3 Diritto alla riservatezza e protezione dei dati personali

Il diritto alla riservatezza presenta delle differenze rispetto al diritto alla protezione dei dati personali.

Il primo è un diritto a contenuto *negativo*[26]: ovvero permette di escludere i terzi dalla conoscenza di informazioni riservate che riguardano la vita privata. Lo schema è dunque quello dello *ius excludendi alios*[27]:

---

[25] V. CATAUDELLA A., *La tutela civile della vita privata*, Milano, Giuffrè, 1972, pp. 33 ss.: "*Quando si considera la libertà in esso garantita si è naturalmente portati a pensare alla sua estrinsecazione positiva, cioè alla libertà di diffondere, comunicandolo ad altri, quello che si pensa. Ma un aspetto non meno importante è* […] *quello negativo.*
Un aspetto di questa libertà negativa, con riguardo alla manifestazione del pensiero […] [è] *la libertà di non dover dire quello che si pensa.*
Altro aspetto […] *è la libertà di tacere: cioè di non manifestare il proprio pensiero. Libertà com'è logico, non significa solo potere di scegliere tra il tacere del tutto ed il manifestare il proprio pensiero ma comporta anche, nel caso che il soggetto si decida a manifestare il proprio pensiero, il potere di limitarne l'ambito di diffusione, cioè la libertà di «manifestare il proprio pensiero ad alcuni e non ad altri».*
Ma se così è, ne discende, mi pare, che tutti i comportamenti di estranei, volti a capire un pensiero che il soggetto non intende manifestare (e per questo abbiamo visto che deve intendersi anche la mera notizia di fatti), oppure a diffonderlo oltre la cerchia di persone cui egli lo aveva destinato, ledono la sua libertà negativa di manifestazione del pensiero".
Per una critica v. AULETTA T., *Riservatezza e tutela della personalità*, Milano, Giuffrè, 1978, pp. 91 ss.: "*Tale dottrina parte da una constatazione indubitabile nel senso che la libertà di pensiero garantisce non solo la libera circolazione del pensiero (aspetto positivo della libertà) ma anche la libertà di tacere (aspetto negativo della libertà). Più dubbiosi può lasciare un secondo passaggio, secondo il quale la libertà di tacere verrebbe violata da «tutti i comportamenti… volti a carpire un pensiero che il soggetto non intende manifestare… oppure diffonderlo oltre la cerchia di persone cui egli lo aveva destinato» (ed è proprio sulla fondatezza dell'ultima proposizione che può sorgere il dubbio).*
Se la tesi prospettata, come pare, un obbligo generale di segreto, è da osservare che lo stesso è estraneo al nostro ordinamento, dove la tutela assoluta del segreto è limitata alle vicende lesive dell'onore e del decoro, ed incide sulla libertà positiva di pensiero, che rimarrebbe gravemente condizionata dall'impossibilità di rivelare notizie anche da privato a privato non aventi rilevanza sociale. Ma, soprattutto, ci pare si esorbiti dal concetto dal concetto storicamente consolidato di libertà, infatti, l'ordinamento tende a garantire all'individuo un ambito nel quale compiere scelte discrezionali senza la diretta ingerenza di terzi, tende cioè a non imporre scelte o comportamenti non graditi ed a non impedire scelte o comportamenti voluti. […]".
Per una visione più ampia sul tema v. anche RUFFINI GANDOLFI M. L., *Diritto alla riservatezza*, in *Digesto delle discipline privatistiche*., sez. civ., Torino, 1990, vol. VI, pp. 69 - 77, anche in https://onelegale.wolterskluwer.it/document/diritto-alla-riservatezza/94GI0000000334?searchId=615907269&pathId=f5a68c6b795de&offset=0#nota_11.

[26] Cfr. FINOCCHIARO G., *Privacy e protezione dei dati personali: disciplina e strumenti operativi*, Torino, Zanichelli editore, 2016 (I ed. 2012), p. 8.

[27] Dal latino: "*diritto di escludere tutti gli altri*". L'espressione è tipicamente utilizzata in riferimento al diritto alla proprietà privata.

si escludono dalla conoscenza/fruizione del bene[28] oggetto del diritto i soggetti che non ne siano il titolare del diritto[29].

Il diritto alla protezione dei dati personali è, invece, un diritto a contenuto *positivo*; ha cioè la finalità di permettere al titolare di avere il controllo sui propri dati personali[30]. Già a questo punto si delinea il primo problema: come è possibile far in modo che un soggetto mantenga un controllo attivo su un'informazione che viene generata, gestita e conservata lontano da lui?

In realtà quasi nessuno si era posto questo quesito fino agli anni '70 del secolo scorso: fino ad allora infatti i dati personali venivano raccolti in quantità e con frequenza ben inferiori rispetto ad oggi[31], erano conservati in polverosi archivi cartacei, la cui consultazione era molto dispendiosa[32]. Soprattutto però, questa memoria era "*distribuita*": ovvero divisa sul territorio tra tutti gli enti e le aziende che avevano raccolto informazioni, era quindi impossibile collegare le varie infrastrutture[33]. Non vi era motivo di ritenere tutto ciò una minaccia alla personalità individuale e quindi anche la disciplina giuridica non era particolarmente sviluppata[34].

1.1.4 Le banche dati informatiche e le prime leggi sulla gestione dei dati

Nonostante le esperienze degli Stati totalitari e della Seconda guerra mondiale, l'idea di inserire il diritto alla protezione dei dati personali nelle Costituzioni non si affermò immediatamente. Infatti, nessuna delle Costituzioni europee emanate poco dopo la guerra tutelava separatamente il diritto alla riservatezza e il rispetto della vita privata[35]. Ciò è legato al fatto che tali carte fondamentali furono stilate da una classe politica formata

---

[28] Oggi i dati personali sono classificabili a tutti gli effetti come beni; v., ad esempio, MANTELERO A., *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati*, cit., pp. 294 s.

[29] Cfr. TORRE M., *Protezione dei dati personali, processo penale e intercettazioni*, in *Diritto penale e processo*, 2/2019, pp. 180-187, in http://hdl.handle.net/2158/1151885 e in https://studiolegale.leggiditalia.it/#id=10AR0000242721ART2,__m=document, p. 180.

[30] La definizione di "dato personale" è stata modificata dai vari *corpus* legislativi che si sono susseguiti (v. *infra*, cap. 1, § 1.2.3). Cfr. FINOCCHIARO G., *Privacy e protezione dei dati personali: disciplina e strumenti operativi,* cit., pp. 8 s.

[31] Sebbene non sia possibile effettuare un conteggio della totalità dei dati personali raccolti in Europa dell'epoca, è comunque vero che tale numero risulta irrisorio se confrontato con i *big data* a cui siamo abituati oggi. V. LOVATI M., *Quanto sono grandi i big data?* in *Data manager online*, 14 giugno 2018, https://www.datamanager.it/2018/06/quanto-sono-grandi-i-big-data/.

[32] Cfr. FINOCCHIARO G. & AL., *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2020, pp. 288 s.

[33] *Ibidem*.

[34] V. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali*, cit., pp. 56 ss.

[35] *Ibidem*.

per la maggior parte da persone che erano state sconfitte e perseguitate dai totalitarismi o che avevano fatto parte delle varie resistenze. Tutte queste personalità erano però accomunate dal non avere un'adeguata consapevolezza dell'evoluzione tecnica dei mezzi elettronici[36].

In Europa le prime normative sulla protezione dei dati vennero emanate negli anni '70, quando l'informatizzazione degli archivi cartacei era giunta ad uno stadio avanzato e ormai noto ai decisori politici[37]. L'informatizzazione non solo rese più veloce l'accesso alle informazioni, ma gettò le basi per collegare tutti quei dati che fino ad allora erano fisicamente distribuiti in luoghi diversi[38].

Ciò concorse, come riporta il giurista Giovanni B. Ferri in riferimento alla teoria del politologo Nicola Matteucci[39], a far sì che la privacy diventasse un problema rilevante e riconosciuto dai cittadini europei e questo per tre motivi. Il primo, come abbiamo visto, è di tipo storico e riguarda la precedente esperienza del totalitarismo[40], in cui la separazione tra "*pubblico e privato è sfociata nella generale politicizzazione di ogni momento dell'esistenza umana*"[41]. Il secondo perché, dove anche il totalitarismo non fosse giunto nelle sue forme più estreme, lo stato sociale aveva assorbito sia la sfera privata che la sfera pubblica, generando un conformismo di massa[42]. Il terzo motivo riguarda, come abbiamo già ampiamente illustrato, il diffondersi di nuove tecnologie che, in mano al pubblico o al privato, "*producono strumenti sempre più sofisticati, di penetrazione e di controllo della vita privata altrui,* […] *mass media,* […] *l'affermarsi delle cosiddette banche dei dati.* […] *Tutto ciò ha determinato un vero assault on privacy e cioè dell'individuo*"[43]. Per dare una

---

[36] *Ibidem.* Si pensi ad esempio alle tutele della nostra Costituzione per quanto riguarda la libertà d'espressione. Queste si riferiscono solo alla stampa, sebbene già all'epoca radio e cinematografia erano diffuse ed avevano avuto un ruolo fondamentale nella propaganda fascista (*ibidem*).

[37] Cfr. FINOCCHIARO G. & al., *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, pp. 289 s.

[38] *Ibidem.*

[39] Cfr. MATTEUCCI N., *Introduzione: pubblico e privato,* in *Privacy e banche dati*, Bologna, Il Mulino, 1981, p. 22, cit. da FERRI G.B., *Privacy e libertà informatica*, in ALPA G. & BESSONE M. (a cura di), *Banche dati telematica e diritti della persona*, Padova, Cedam, 1984, pp. 46 ss. È importante sottolineare che ogni singola motivazione ha avuto un'importanza fondamentale nell'avvio del processo di legiferazione in materia di banche dati. Si pensi, ad esempio, agli anni '50, quando era sicuramente vivo il ricordo dell'esperienza totalitaria, ma ancora non si era sviluppato il progresso tecnologico, e infatti si dovette aspettare circa 20 anni per le prime leggi in materia di banche dati.

[40] V. nota n. 8, p. 2.

[41] FERRI G.B., *Privacy e libertà informatica,* cit*.,* p. 46.

[42] *Ibidem*.

[43] *Ivi*, pp. 46 s.

dimensione del fenomeno, solo in Italia, secondo una rilevazione governativa del 1981[44], le aziende che possedevano, o che utilizzavano, una o più banche dati ad elaborazione elettronica erano quasi trecentomila.

La prima legge che, in Europa, regolò l'utilizzo delle banche dati è una legge locale del Land dell'Assia della Germania Federale del 1970, con lo scopo di tutelare esplicitamente le persone, e in particolare i lavoratori, da schedature indebite, regolando il trattamento dei dati all'interno degli archivi informatici[45]. Questo provvedimento aveva un fortissimo valore politico, perché l'Assia faceva all'epoca parte della Repubblica Federale di Germania, a ovest del Muro e nella sfera d'influenza della NATO, contrapposta alla Repubblica Democratica Tedesca che era sotto l'influenza di Mosca. Dunque, che un Land della Germania Ovest regolasse il trattamento dei dati personali e limitasse le schedature di massa aveva un forte valore in contrapposizione alle idee di democrazia[46] tipiche della Germania Est, basate su forme di controllo tradizionali ed informatiche che in quel Paese si praticavano ampiamente[47].

Nello stesso anno, in Francia venne approvata la l. 17 luglio 1970, n. 70 - 643, che riconobbe il "*droit a la vie privée*" (art. 22). Tale norma fu poi aggiornata con la l. 6 gennaio 1978, n. 17, il cui art. 1 recitava: "*L'informatique doit être au service de chaque citoyen. […] ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques*"[48]. Venne inoltre istituita la *Commission Nationale de l'Informatique e des Libertes* (art. 6), deputata a controllare che fosse rispettate le disposizioni contenute nella medesima legge[49].

In ambito nazionale, la prime legge di uno Stato europeo riguardante esplicitamente i dati personali e le banche dati fu il *Data Act* svedese del 1973: questa legge non conteneva alcuna istruzione su come vadano gestiti e

---

[44] *Relazione sulla rilevazione effettuata al 31 dicembre 1981 in ordine alla formazione e detenzione di archivi magnetici contenenti dati o informazioni su cittadini italiani* (art. 8, ult. comma della legge 1° aprile 1981, n. 121), presentata dal Presidente del Consiglio dei Ministri alla Presidenza della Camera dei Deputati il 31 gennaio 1983, in Camera dei Deputati – *Atti Parlamentari (VIII legislatura),* Roma 1983, pp. 29 ss (v. *infra*).

[45] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati*, cit., p. 59.

[46] La parola "democrazia" è qui impropria e si riferisce al nome ufficiale della Germania Est. Per una panoramica sugli elementi fondanti di uno Stato democratico si rinvia a TONELLO F., *Democrazie a rischio. La produzione sociale dell'ignoranza*, Milano Torino, Pearson, 2019.

[47] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati*, cit., p. 59.

[48] "*L'informatica deve essere al servizio dei cittadini […] non deve attentare né all'identità umana, né ai diritti dell'uomo, né alla vita privata*", trad. *ibidem*.

[49] *Ibidem.*

processati i dati personali, né indicazioni sui principi della *data protection*[50]. Ciò che il *Data Act* sancì fu che l'attività di ogni registro di raccolta di dati personali dovesse essere approvata preventivamente da un'autorità governativa creata ad hoc: il *Data Inspection Board*[51]. Un dettaglio interessante di questa normativa è il fatto che essa prevedeva una speciale autorizzazione per archivi contenenti informazioni relative a provvedimenti per cure disintossicanti, per ricoveri psichiatrici e per terapie destinate a persone diversamente abili[52]: cioè di dati che oggi consideriamo *sensibili*[53].

Inoltre, il *Data Act* introdusse un tema ancora oggi di stringente attualità: lo scambio dei dati sul piano internazionale, conosciuto anche come *flusso transfrontaliero dei dati*[54]. Per comprendere l'ampiezza del tema si pensi anche alla sola ricerca scientifica e al giornalismo, in cui questo tipo di trattamento è addirittura essenziale per lo svolgimento di queste attività[55].

Un'altra legge importante è stata il *German Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG)* emanata dalla Repubblica Federale Tedesca nel 1977, il quale affondava le proprie radici, sia come contenuti sia come significato politico, nella legge del Land dell'Assia di cui sopra[56]. A differenza del *Data act* svedese, nella legge tedesca possiamo trovare alcuni elementi qui rilevanti, che saranno ripresi dal *corpus* normativo europeo che vedremo in seguito[57]: ad esempio la definizione di dato personale come "*informazioni personali o su circostanze materiali riguardanti un soggetto fisico identificato o identificabile*"[58]. È però importante

---

[50] Quelli che oggi chiameremmo "fondamenti giuridici del trattamento" e "condizioni di liceità del trattamento". V. OMAN S., *Implementing Data Protection in Law*, in *Scandinavian Studies in Law*, vol. 47, 2004, pp. 389 - 403, in https://scandinavianlaw.se/pdf/47-18.pdf.

[51] *Ibidem*.

[52] Cfr. FROSINI V., *Riservatezza e calcolatori* in *Banche dati telematica e diritti della persona*, Padova, Cedam, 1984, pp. 40 ss.

[53] La definizione di "*dati sensibili*" è da riferirsi al *Codice in materia di protezione dei dati personali*, d.lgs. 30 giugno 2003, n. 196, (c.d. Codice privacy). Tale definizione è stata introdotta nel nostro ordinamento dall'art. 22, l. 31 dicembre 1996, n. 675, sostituita in seguito dal Codice privacy. Si tratta di quelle tipologie di dati individuate ora dall'art. 9 del Regolamento Europeo 679/2016 - *General Data Protection Regulation*, (Regolamento o GDPR).

[54] Eng. *Transborder data flow*.

[55] Cfr. FROSINI V., *Riservatezza e calcolatori* in *Banche dati telematica e diritti della persona*, cit., pp. 40 ss.

[56] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati*, cit., p. 60.

[57] V. *infra*, cap. 1, § 1.2.3.

[58] La traduzione dal tedesco all'inglese è in RICCARDI J., *The German Federal Data Protection Act of 1977: Protecting the right to Privacy?,* in *Boston College International and Comparative Law Review*, Vol 6, I 1, 1983, in https://core.ac.uk/download/pdf/80399406.pdf, p. 249 che costituisce anche dottrina di riferimento per questa parte di testo. Quella nel testo è una traduzione autonoma di chi scrive.

sottolineare che il *BDSG* non proteggeva i dati personali in quanto beni che necessitano protezione, ma in quanto la loro tutela era strumentale alla protezione della riservatezza dei soggetti interessati. Per questo motivo non troviamo nel *BDSG* alcuna protezione per i dati che riguardano persone non fisiche, come aziende o enti, né una differenziazione tra le varie tipologie di dati[59], come invece avviene oggi per i *dati sensibili*[60].

Venendo ora alla situazione italiana, il primo testo normativo che disciplinò, in modo ancora embrionale, il trattamento dei dati fu la l. 1° aprile 1981, n. 21 – *Amministrazione della pubblica sicurezza e coordinamento delle forze di polizia*, che ha introdotto il nuovo Centro di elaborazione dei dati del Ministero dell'Interno. In particolare, l'art. 8, comma 3° così recita: "*Ogni amministrazione, ente, impresa, associazione o privato che per qualsiasi scopo formi e detenga archivi magnetici nei quali vengano inseriti dati o informazioni di qualsivoglia natura concernenti cittadini italiani, è tenuta a notificare l'esistenza dell'archivio al Ministero dell'interno entro il 31 dicembre 1981.* […] *Entro il 31 dicembre 1982 il Governo informerà il Parlamento degli elementi così raccolti ai fini di ogni opportuna determinazione legislativa a tutela del diritto alla riservatezza dei cittadini*"[61]. Non si tratta evidentemente di una vera e propria regolamentazione in materia di banche dati e archivi elettronici, ma costituisce il primo passo compiuto dal nostro Paese sul tema[62].

1.1.5 Convenzione "di Strasburgo": n. 108 del 1981

Nel 1981 venne emanata dal Consiglio d'Europa la Convenzione n. 108, altresì nota come Convenzione di Strasburgo[63]. Non è un caso che essa sia stata approvata quattro anni dopo il *BDSG* tedesco; nel decennio precedente, come abbiamo visto[64], alcuni Stati europei si erano dotati di leggi riguardanti, con modi e fini

---

[59] Cfr. *ivi*, pp. 243 - 271.

[60] V. n. 53, p. 9.

[61] L. 1° aprile 1981, n. 121., art. 8, comma 3°, testo integrale in https://www.foroplus.it/visualizza.php?sha1=6fe635afa0c35d9865fc07714609d3bd0c8c92b2. Il comma 3° del suddetto articolo è stato abrogato dall'art. 43, comma 1°, della l. 31 dicembre 1996, n. 675 (la prima legge sulla privacy italiana che recepisce la precedente Direttiva europea n. 95/46/CE).

[62] Cfr. FROSINI V., *Riservatezza e calcolatori* in ALPA G. & BESSONE M. (a cura di), *Banche dati telematica e diritti della persona*, cit., p. 42.

[63] Convenzione 28 gennaio 1981, n. 108. Per il testo completo della Convenzione v. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078c45.

[64] V. *supra,* cap. 1, § 1.1.4.

diversi, la tutela dei dati personali[65]. Queste leggi nazionali[66] presentavano spesso elementi di incompatibilità tra di loro e la Convenzione di Strasburgo rappresentava pertanto anche un tentativo di coordinarle[67]. Inoltre, nel 1981 l'informatica era già diventata un fenomeno "di massa": se da un lato gli strumenti tecnici informatici delle aziende e degli enti pubblici continuavano ad evolversi, dall'altro le persone iniziavano ad avere i primi *personal computer* nelle proprie case, prima più complessi nell'utilizzo, poi via via sempre più semplici[68].

Lo scopo principale della Convenzione era dunque quello di "*garantire, sul territorio di ogni Parte, ad ogni persona fisica, qualunque sia la sua cittadinanza o residenza, il rispetto dei diritti e delle libertà fondamentali, ed in particolare del diritto alla vita privata, nei confronti dell'elaborazione automatizzata dei dati di carattere personale che la riguardano (protezione dati)*"[69].

L'importanza della Convenzione sta inoltre nell'aver introdotto una serie di definizioni a livello sovranazionale[70]. La prima riguarda i dati personali: "*per 'dati personali' si intende ogni informazione relativa a una persona fisica identificata o identificabile (persona interessata)*"[71]. Altri elementi rilevanti sono le condizioni di liceità sulla qualità dei dati (art. 5), la definizione di particolari categorie di dati[72] (art. 6) e la definizione dell'insieme delle "*Garanzie supplementari per la persona interessata*", tra le quali troviamo: il diritto dell'interessato a conoscere l'esistenza dei dati che lo riguardano, il diritto di rettifica e il diritto ad ottenere la cancellazione dei dati qualora questi siano stati ottenuti in modo illecito (art. 8).

Un ulteriore elemento di grande rilevanza è il principio di libera circolazione dei dati personali, introdotto dall'art. 12, che sarà uno degli elementi fondanti del ben più recente GDPR[73].

Non è questa la sede per una trattazione approfondita della Convenzione; tuttavia, si ritiene che quanto detto

---

[65] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati,* cit., pp. 60 ss.

[66] *Ibidem.*

[67] *Ibidem.*

[68] Cfr. AA.VV. *Come si è arrivati al GDPR: dalla privacy al Regolamento*, tratto da un intervento di Pizzetti F., in *Privacy Lab (Tinexta Group)*, 30/06/2020, con aggiornamento del 03/03/2022, in https://www.privacylab.it/IT/989/come-si-e-arrivati-al-gdpr-dalla-privacy-al-regolamento/.

[69] Art. 1, Conv. 1981, n. 108.

[70] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati,* cit., p. 61.

[71] Art. 2, lett. a, Convenzione di Strasburgo. Nello stesso articolo trovano spazio anche le definizioni di: "*collezione automatizzata di dati*", "*trattamento automatizzato*", "*detentore di una collezione di dati*", che non riportiamo per brevità.

[72] Quelli che oggi chiamiamo "*dati sensibili*", v. nota n. 53, p. 9.

[73] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati,* cit., pp. 62 s.

basti a far comprendere il valore, non solo giuridico, che questo testo normativo ha avuto nell'evoluzione della tutela dei dati personali in Europa[74]. In un certo senso, si può dire che la Convenzione di Strasburgo segna uno spartiacque dopo il quale il trattamento delle informazioni personali non può avvenire senza adeguate garanzie[75]. Inoltre, come vedremo tra pochissimo, essa costituisce la base del quadro concettuale che caratterizza l'attuale legislazione europea.

1.2 La Direttiva madre (1995)

Prima di proseguire è opportuno ricordare che la Convenzione n. 108, di cui abbiamo parlato[76], fu adottata dal Consiglio d'Europa, un'organizzazione internazionale distinta dalla Comunità Europea (CE), ora Unione Europea[77]. Quindi quest'ultima, tra i cui scopi fondamentali vi è appunto quello di armonizzare il quadro normativo europeo su una serie di tematiche, era sprovvista di una regolazione comune in tema di riservatezza ancora all'inizio degli anni '90[78].

L'atto normativo della CE in materia di dati personali venne approvato nel 1995 e, ancora una volta, per comprenderne appieno le motivazioni è necessario osservare il contesto storico-normativo entro cui è stato emanato. Infatti, nel 1993 è entrato in vigore il Trattato di Maastricht, cui abbiamo appena accennato[79], con il quale la CE si impegnava in modo definitivo ad attuare il Mercato Unico in ambito europeo[80].

Le conseguenze di tale impegno che qui interessano sono essenzialmente due: la prima è la cessazione di ogni controllo per le merci in movimento tra gli Stati della CE[81]; la seconda è l'abbattimento dei controlli di frontiera

---

[74] *Ivi,* p. 63.

[75] *Ibidem*.

[76] V. *supra*, cap. 1, § 1.1.5.

[77] Cfr. AA.VV. *Come si è arrivati al GDPR: dalla privacy al Regolamento*, tratto da un intervento di Pizzetti F. in *Privacy Lab (Tinexta Group)*, 30/06/2020, con aggiornamento del 03/03/2022. Il Trattato di Maastricht, firmato dai dodici paesi allora membri, il 7 febbraio 1992, ha sancito la trasformazione della Comunità Economica Europea in Unione Europea.

[78] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati*, cit., p. 64.

[79] V. nota n. 77, p. 12.

[80] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati,* cit., p. 64.

[81] Tale fatto si verifica direttamente all'entrata in vigore del Trattato, dal 1° gennaio 1993.

anche per le persone, come conseguenza dell'Accordo di Schengen[82], al quale man mano aderirono, negli anni '90, tutti i Paesi CE[83].

Quindi, per fare in modo che l'abbattimento delle frontiere fisiche avesse una completa efficacia, era necessario superare anche le frontiere immateriali, costituite dalle diverse leggi nazionali in tema di dati personali. Per questo motivo si assistette, all'inizio degli anni '90, all'avvio delle trattative che portarono all'emanazione della Direttiva 95/46/CE del 24 ottobre 1995 (in seguito, 'Direttiva')[84].

1.2.1 La forma giuridica della Direttiva

Per comprendere le finalità della Direttiva 95/46/CE è bene analizzare dapprima lo strumento normativo.

Le direttive, a differenza dei regolamenti, non sono indirizzate a tutti i cittadini dell'Unione, ma sono destinate agli Stati, nei confronti dei quali sono vincolanti[85]. La direttiva si distingue dal regolamento perché questa è un *mezzo normativo indiretto*, avente cioè il solo effetto di imporre degli obiettivi ai quali gli Stati devono adeguarsi, adottando atti normativi finalizzati a tale scopo. Ogni Stato mantiene quindi una certa discrezionalità, variabile a seconda delle situazioni, sul modo in cui modificare la propria legislazione nazionale per raggiungere gli obiettivi individuati dalla direttiva[86].

In questo senso, le direttive vengono spesso utilizzate non con il fine di imporre una regola sovranazionale, ma al fine di armonizzare, su un determinato tema, le diverse legislazioni nazionali, tra le quali si sono generati profili di incompatibilità[87].

In questo caso, il primo effetto della Direttiva 95/46/CE fu però quello del mutuo riconoscimento: ovvero il fatto che, nell'ambito dello scambio di dati tra Paesi appartenenti alla CE, si applicasse la legge del Paese dove

---

[82] Il nome ufficiale è *Accordo fra i governi degli Stati dell'Unione economica del Benelux, della Repubblica federale di Germania e della Repubblica francese relativo all'eliminazione graduale dei controlli alle frontiere comuni*. È un trattato internazionale firmato a Schengen il 14 gennaio 1985 inizialmente da Belgio, Paesi Bassi, Lussemburgo, Francia e Germania Ovest; avente come conseguenze l'abbattimento dei controlli alle frontiere per merci e persone. L'accordo è stato via via esteso ad altri stati della CE ed è stato poi integrato al Trattato di Maastricht dal successivo Trattato di Amsterdam del 1999.

[83] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati,* cit., p. 65.

[84] *Ibidem*.

[85] V. ZANGHÌ C., *Istituzioni di diritto dell'Unione Europea*, Torino, Giappichelli, IV ed., 2003, p. 270.

[86] Tale processo è chiamato "ricezione della direttiva". *Ibidem.*

[87] *Ibidem.*

è stabilito il responsabile[88] del trattamento. Questo elemento è estremamente rilevante perché costituisce la rinuncia da parte della CE di giungere a una regolazione vincolante comune, obiettivo che era stato perseguito nei cinque anni di trattative che avevano preceduto l'approvazione della Direttiva[89].

Tornando al contesto normativo, le direttive europee necessitano, come abbiamo detto, di essere recepite dai singoli Stati, che devono attuarle conformando le proprie legislazioni nazionali. A partire dal 1996, la CE impose la ricezione della Direttiva 95/46/CE come condizione non negoziabile per aderire all'Accordo di Schengen[90]. Risulta quindi chiaro che, nel quadro della Comunità Europea degli anni '90, la Direttiva 95/46/CE ebbe un ruolo principalmente strumentale, finalizzato all'abbattimento delle frontiere interne alla Comunità[91].

1.2.2 Il concetto di "rischio" nella Direttiva 95/46

Come abbiamo già detto, il rapporto tra evoluzione informatica e tutela dei dati personali è molto stretto. In particolare, la disciplina della *data protection* si è sviluppata in funzione del rischio dettato dalla possibilità di commettere abusi, via via diversi, nell'utilizzo dei dati attraverso l'elaborazione elettronica[92].

Più precisamente, prima è nata l'istanza sociale di porre un freno al nuovo potere informatico e in seguito sono state emanate le norme legate alle dinamiche del paradigma tecnologico, con riferimento ai rischi potenziali per la società. Ciò che mancava in queste prime normative era un "*riferimento al ruolo dell'interessato in termini di pieno esercizio dell'autodeterminazione rispetto alle informazioni che lo riguardano*"[93].

Il rischio legato al trattamento delle informazioni personali non è però statico, specie a fronte di un'evoluzione continua dei processi di acquisizione e trattamento che ha portato i dati ad avere un ruolo fondamentale nell'avvento del *direct marketing* e, più in generale, nella produzione di prodotti e servizi personalizzati da parte di industrie private[94].

---

[88] Per "responsabile" si intende al soggetto individuato all'art. 2 della Direttiva 94/46/CE.

[89] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati*, cit., pp. 66 s.

[90] V. nota n. 82, p. 13.

[91] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati*, cit., p. 67.

[92] Cfr. MANTELERO A. *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati*, in FINOCCHIARO G. (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Torino, Zanichelli, 2017, p. 293.

[93] *Ibidem.*

[94] *Ivi*, pp. 294 s.

È così che la c.d. "*sindrome del pesce rosso*"[95] ha lasciato spazio all'idea che i dati personali abbiano anche un valore economico, in quanto fondamentali per programmare strategia di produzione e vendita efficaci. L'interessato non è quindi più stato visto solamente come un soggetto passivo da proteggere, ma come il proprietario di una "*nuova ricchezza costituita dal patrimonio informativo che lo riguarda*"[96].

È per questo motivo che la disciplina dei dati personali si evolve, a partire dagli anni '90, riconoscendo un ruolo più centrale all'interessato e introducendo il "consenso" come fondamento giuridico necessario al trattamento delle informazioni che riguardano gli individui[97]. In questo modo, non solo si lega la discrezionalità della gestione dei dati alla personalità dell'individuo, ma si "liberalizza", il "*consapevole sfruttamento economico degli attributi della personalità*"[98]. Di riflesso, grazie all'introduzione del consenso, si assiste ad un incremento dello sfruttamento economico delle informazioni personali, che permettono lo sviluppo di nuove banche dati e di flussi di informazioni sempre più efficienti.

Naturalmente però, l'interessato che acconsente al trattamento dei suoi dati deve farlo conoscendo le conseguenze della propria decisione, ovvero sapendo da chi e in che modo verranno trattati. A questo proposito si inizia, in questa fase, a parlare di "consenso informato", nel quale, attraverso un'informativa, si esplicita all'interessato chi tratterà i suoi dati, in che modo e per quali finalità. Tutto ciò permette a chi cede i propri dati di valutare i vantaggi e gli svantaggi della decisione o, per ricollegarci al nostro discorso, di comprendere i rischi che ne derivano[99].

Ad essere rilevante non è più solo il rischio collettivo, relativo alla società nel suo insieme, tenuta sotto controllo attraverso le banche dati, ma assume importanza anche il rischio individuale, derivante dal trattamento dai dati disaggregati che riguardano una persona specifica[100].

Inoltre, il rischio legato al singolo può essere a sua volta scisso in due metà: da un lato troviamo un rischio che

---

[95] Si tratta di un'espressione, originaria dei Paesi scandinavi, che indica la sensazione dei cittadini di essere completamente esposti all'occhio indagatore dei governi, come dei pesci rossi in un aquario. *Ivi*, p. 294.

[96] MANTELERO A. *Il nuovo approccio della valutazione del rischio*, cit., p. 294.

[97] Naturalmente ciò non significa che lo Stato abbia abbandonato, nel corso di questa evoluzione, il suo ruolo di "garante" della tutela dei diritti dei cittadini, specialmente se si considera che il progresso tecnologico ha portato alla creazione di strumenti e meccanismi che difficilmente possono essere compresi dal comune cittadino. Cfr. *ivi*, p. 294 s.

[98] Cfr. MANTELERO A. *Il nuovo approccio della valutazione del rischio*, cit., p. 296.

[99] *Ivi*, pp. 297 s.

[100] *Ibidem*.

possiamo definire "lecito", costituito dalle possibili conseguenze sgradite all'interessato dei trattamenti che, regolarmente consentiti, non contrastano di per sé con la normativa in materia. Dall'altro lato abbiamo invece un rischio propriamente illecito, ovvero derivante da trattamenti illeciti dei dati, di cui risponde il responsabile[101] del trattamento[102].

Delle due parti del rischio che abbiamo appena illustrato, è la seconda ad essere presa in maggior considerazione nella Direttiva 95/46 CE, la quale prescrisse una serie di misure, di natura organizzativa o tecnica, variabili a seconda del livello di rischio, la cui adozione autorizzava la raccolta e il trattamento dei dati. La Direttiva delegò, invece, *in toto* all'interessato la gestione del rischio che abbiamo definito lecito[103]. Questa idea di controllo sui dati demandato al singolo presupponeva che quest'ultimo sia consapevole delle conseguenze e dei rischi che derivano dalla gestione dei propri dati personali[104], presupposto su cui l'Unione sarebbe tornata non molti anni dopo.

1.2.3 I principali contenuti della Direttiva

Dopo aver fissato i principi generali di protezione dei dati personali e di libera circolazione degli stessi (art. 1), la Direttiva fornì, all'art. 2, le definizioni di dato personale[105], di trattamento dei dati personali[106], di responsabile del trattamento[107] e di consenso[108] della persona interessata[109]. Vennero poi sanciti i diritti dell'interessato e le condizioni di liceità di trattamento, dei quali non ci occuperemo[110].

Rilevante ai fini del nostro percorso è, invece, l'obbligo di istituzione di un'Autorità nazionale indipendente adibita a "*sorvegliare, nel suo territorio, l'applicazione delle disposizioni di attuazione della presente direttiva,*

---

[101] Per "responsabile" si intende al soggetto individuato all'art. 2 della Direttiva 94/46/CE.

[102] Cfr. MANTELERO A., *Il nuovo approccio della valutazione del rischio*, cit., pp. 297 s.

[103] *Ibidem.*

[104] *Ivi*, pp. 298 - 305.

[105] "*Qualsiasi informazione concernente una persona identificata o identificabile*", art. 2, Direttiva 95/46/CE.

[106] "*Qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate ai dati personali*", art. 2, Direttiva 95/46/CE.

[107] "*La persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento dei dati personali*", art. 2, Direttiva 95/46/CE.

[108] "*La manifestazione di volontà specifica e informata della persona interessata che autorizza a trattare dati personali che la riguardano*", art. 2, Direttiva 95/46/CE.

[109] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati*, cit., pp. 75 s.

[110] Per una generale ma accurata visione sui contenuti della Direttiva: v. *ivi* pp. 77 - 112.

adottate dagli Stati membri. Tali autorità sono pienamente indipendenti nell'esercizio delle funzioni loro attribuite"[111], a cui venne dedicata buona parte del Capo VI della Direttiva.

Le Autorità nazionali vennero definite "*indipendenti*": è un aspetto centrale, in quanto esse sono chiamate a controllare che la Direttiva venga applicata sia da parte dell'amministrazione e dei privati, sia rispetto alla legislazione e la regolazione dello Stato in cui operano[112].

Tra i poteri che la Direttiva attribuì alle Autorità nazionali troviamo: "*poteri investigativi, come il diritto di accesso ai dati oggetto di trattamento e di raccolta di qualsiasi informazione necessaria all'esercizio della sua funzione di controllo*"[113]; si tratta di una facoltà estremamente importante, che consente loro di effettuare qualunque verifica su qualunque trattamento effettuato all'interno della loro zona di competenza[114].

In conseguenza di tali verifiche, le Autorità[115] ottennero (e ancora oggi hanno) "*poteri d'intervento*"; ebbero inoltre la facoltà: "*fornire pareri*" preventivi, *ordinare il congelamento, la cancellazione o la distruzione dei dati*", *"vietare a titolo provvisorio o definitivo il trattamento*", notificare avvisi al responsabile di trattamento, "*adire i Parlamenti o altre istituzioni politiche nazionali*"[116]. Il cerchio venne idealmente chiuso dal paragrafo 4, con il quale si attribuì alle Autorità indipendenti "*il potere di promuovere azioni giudiziarie in caso di violazione delle disposizioni nazionali di attuazione della Direttiva ovvero di adire per dette violazioni alle autorità giudiziarie*"[117].

Per evitare che le Autorità garanti dei diversi Stati operassero in modo non conforme tra loro, l'art. 29 della Direttiva 95/46/CE istituì il *Gruppo europeo per la tutela dei dati personali*[118], formato, tra gli altri, da un

---

[111] Art. 28, Direttiva 95/46/CE.

[112] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati*, cit., p. 117.

[113] Art. 28, par. 3, Direttiva 95/46/CE.

[114] Questo potere è stato, almeno in Italia, in gran parte limitato dal fatto che la norma non dà alcuna indicazione riguardo a quante e quali risorse debbano essere assegnate alle Autorità nazionali, elemento che verrà invece modificato nel Regolamento. Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati*, cit., p. 118.

[115] Continuiamo ad utilizzare il plurale perché l'art. 24, Direttiva 95/46/CE riserva ad ogni Stato la possibilità di creare più di un'autorità indipendente. Tale fattispecie trova applicazione ad esempio in Germania, dove all'Autorità centrale si affiancano le Autorità dei singoli Land. Inoltre, si ricorda che è comune riferirsi all'Autorità nazionale italiana con i termini "Autorità Garante per la privacy" o semplicemente "il Garante privacy".

[116] Art. 28, par. 3, Direttiva 95/46/CE (tutti i virgolettati nelle quattro righe precedenti).

[117] Art. 28, par. 4, Direttiva 95/46/CE.

[118] Il nome viene spesso abbreviato il Gruppo articolo 29 o, in inglese, *Working Party 29*, da cui deriva anche la sigla WP29. Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati*, cit., p. 121.

rappresentante dell'Autorità di controllo (o dal rappresentante che più Autorità, per i Paesi che ne istituirono più d'una, avessero designato) di ciascuno Stato in cui si applica la Direttiva (art. 29, par. 2[119]). Anche il WP29 era indipendente da ogni Istituzione europea, adottava un proprio Regolamento interno ed era guidato da un Presidente eletto tra i membri, il quale aveva il compito di stilare l'agenda di lavoro (art. 29, par. 7).

In realtà, già da molti anni il Gruppo ha ampliato la sua autonomia e ha iniziato a programmare il suo lavoro annualmente, pubblicandone il piano sul proprio sito ufficiale[120]; ciò non impedisce che talvolta siano trattate questioni urgenti anche se non in programma, spesso suggerite dalla stessa Commissione Europea[121].

L'importanza del WP29 risiede nel "ruolo proattivo" che ha svolto negli anni, agendo da motore della Commissione e rendendosi guida delle singole Autorità nazionali; tale ruolo ha portato il Gruppo a sfruttare al massimo i poteri e il tessuto normativo della Direttiva, riuscendo, ad esempio, a definire l'applicazione di norme pensate per una realtà precedente anche ai continui sviluppi della rete[122]. La conseguenza di ciò è il valore che i suoi documenti e, soprattutto, i suoi pareri hanno raggiunto nel tempo, alcuni dei quali hanno anticipato le principali novità normative dell'Unione[123].

---

[119] "*Il gruppo è composto da un rappresentante della o delle autorità di controllo designate da ciascuno Stato membro e da un rappresentante della o delle autorità create per le istituzioni e gli organismi comunitari, nonché da un rappresentante della Commissione*".

[120] https://edpb.europa.eu/edpb_it. Si ricorda che il nome "*Working Party 29*" è stato modificato in "*European Data Protection Board*" dal GDPR.

[121] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati*, cit., p. 121 s. Si riportano di seguito i compiti del Gruppo articolo 29: "[…] *a) esaminare ogni questione attinente all'applicazione delle norme nazionali di attuazione della presente direttiva per contribuire alla loro applicazione omogenea; b) formulare, ad uso della Commissione, un parere sul livello di tutela nella Comunità e nei paesi terzi; c) consigliare la Commissione in merito a ogni progetto di modifica della presente direttiva, ogni progetto di misure addizionali o specifiche da prendere ai fini della tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di dati personali, nonché in merito a qualsiasi altro progetto di misure comunitarie che incidano su tali diritti e libertà; d) formulare un parere sui codici di condotta elaborati a livello comunitario. 2. Il gruppo, qualora constati che tra le legislazioni o prassi degli Stati membri si manifestano divergenze che possano pregiudicare l'equivalenza della tutela delle persone in materia di trattamento dei dati personali nella Comunità, ne informa la Commissione. 3. Il gruppo può formulare di propria iniziativa raccomandazioni su qualsiasi questione riguardante la tutela delle persone nei confronti del trattamento di dati personali nella Comunità. 4. I pareri e le raccomandazioni del gruppo vengono trasmessi alla Commissione e al comitato di cui all'articolo 31. 5. La Commissione informa il gruppo del seguito da essa dato ai pareri e alle raccomandazioni. A tal fine redige una relazione che viene trasmessa anche al Parlamento europeo e al Consiglio. La relazione è oggetto di pubblicazione. 6. Il gruppo redige una relazione annuale sullo stato della tutela delle persone fisiche con riguardo al trattamento dei dati personali nella Comunità e nei paesi terzi e la trasmette alla Commissione, al Parlamento europeo e al Consiglio. La relazione è oggetto di pubblicazione*." Art. 30, Direttiva 95/46/CE.

[122] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati*, cit., p. 123.

[123] Si pensi, a titolo di esempio, *all'Opinion 3/2010 on the principle of accountability*, riguardante il principio di *accountability*, una delle principali novità del Regolamento 2016/679 UE (v. *infra*, cap. 2), pubblicato dal Gruppo (WP173) il 13/07/2010, ovvero quasi 6 anni prima dell'approvazione definitiva del Regolamento.

1.2.4 Il *privacy officer*

All'Autorità indipendente doveva essere notificata la realizzazione di ogni trattamento che un responsabile[124] mettesse in atto all'interno del territorio di competenza della stessa (art. 18)[125]. Questa era una delle norme più complesse[126], perché conteneva una serie di eccezioni che gli Stati potevano prevedere[127], una delle quali riportava: "*Gli Stati membri possono prevedere una semplificazione o l'esonero dall'obbligo di notificazione soltanto nei casi e alle condizioni seguenti:* […] *qualora il responsabile del trattamento designi, conformemente alla legislazione nazionale applicabile, un incaricato della protezione dei dati*"[128]: è la prima introduzione assoluta del *privacy officer*, precursore del *Data Protection Officer*[129].

L'art. 18 della Direttiva 95/46/CE riportava anche i compiti minimi demandati al *privacy officer*: "*assicurare in maniera indipendente l'applicazione interna delle disposizioni nazionali di attuazione della presente direttiva*"[130] e "*tenere un registro dei trattamenti effettuati dal responsabile del trattamento in cui figurino le informazioni di cui all'articolo 21, paragrafo 2, garantendo in tal modo che il trattamento non sia tale da recare pregiudizio ai diritti e alle libertà della persona interessata*"[131]. Come abbiamo visto però, l'istituzione del *privacy officer* fu rimessa alle legislazioni nazionali, solo poche delle quali, tuttavia, previdero questa figura in fase di ricezione della Direttiva. Tra queste non vi fu l'Italia, il cui Codice privacy non colse questa opportunità[132]. Tale scelta fu vista come segno di una "*certa fatica ad adeguarsi ad una visione della protezione dati attiva e dinamica*"[133] e del fatto che, negli anni '90, nel nostro Paese la privacy fosse vista dai

---

[124] Qui da intendersi con la definizione presente nella Direttiva, v. nota n. 101, p. 16.

[125] "*Gli Stati membri prevedono un obbligo di notificazione a carico del responsabile del trattamento, od eventualmente del suo rappresentante, presso l'autorità di controllo di cui all'articolo 30, prima di procedere alla realizzazione di un trattamento, o di un insieme di trattamenti, interamente o parzialmente automatizzato, destinato al conseguimento di una o più finalità correlate.*" Art. 18, par 1°, Direttiva 95/46/CE.

[126] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati*, cit., p. 98.

[127] Questo è uno degli elementi nei quali i singoli Stati mantengono una certa discrezionalità sul modo in cui adattare la propria legislazione alla Direttiva (v. *supra*, cap. 1, § 1.2.2).

[128] Art. 18, par 2, Direttiva 95/46/CE.

[129] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati*, cit., pp. 3, 4, 98.

[130] Art. 18, par 2, Direttiva 95/46/CE.

[131] *Ibidem.*

[132] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati*, cit., pp. 3, 4, 98.

[133] PIZZETTI F., *Relazione Garante Privacy 2005*, presentata alle Camere il 7 luglio 2006, Doc-Web 1303712, in https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1303712.

più come una burocrazia inutile e un costo superfluo per le imprese e gli enti pubblici[134].

Viceversa Germania, Paesi Bassi, Svezia, Lussemburgo e Francia adottarono il sistema alternativo alla notificazione comprendente il *privacy officer*, proposto dalla Direttiva; inoltre, in Spagna venne introdotta, nel 1999, la figura del *Responsable de seguridad*, "*alla quale il responsabile del trattamento ha formalmente assegnato la funzione di coordinare e controllare le misure di sicurezza applicabili*"[135]. Non si trattava quindi, a differenza di quanto è avvenuto negli altri paesi citati, di una figura che funga da eccezione all'obbligo di notificazione, ma piuttosto di una misura tecnico-organizzativa di sicurezza aggiuntiva per quei trattamenti ritenuti bisognosi di un livello supplementare di tutela[136].

I risultati dell'introduzione del *privacy officer* negli ordinamenti appena citati hanno costituito la base su cui la figura è stata più rigorosamente disciplinata attraverso il successivo regolamento 45/2001/CE e il GDPR. Eccezion fatta per tali esperienze però, molti Stati membri sono rimasti indifferenti all'introduzione del *privacy officer*, tantoché la Commissione Europea ha auspicato "*un ricorso più ampio alle deroghe e, in particolare, alla possibilità contemplata al paragrafo 2 dell'articolo 18 della direttiva, ossia la designazione di un incaricato della protezione dei dati che esonera dall'obbligo di notificazione*" all'interno della prima relazione sull'applicazione della Direttiva, pubblicata nel 2003[137].

---

[134] Cfr. BERNARDI N. & AL., *Privacy officer, la figura chiave della data protection europea. Manuale operativo*, Milanofiori Assago (MI), Ipsoa, 2013, pp. 2 s.

[135] Spa: "*Responsable de seguridad: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y contrlar las medidas de seguridad aplicables*", Art. 2 (*Definiciones*), *Real Decreto 994/1999, por el que se aprueba el Regulmento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal*, testo originale in https://www.boe.es/buscar/doc.php?id=BOE-A-1999-13967, trad. in GRECO A., *La nuova figura del data protection officer (Dpo) nell'Ue*, in *Media laws*. *Rivista di Diritto dei Media*, fasc. 1/2021, pp. 305-307, in https://www.medialaws.eu/rivista/la-nuova-figura-del-data-protection-officer-nellue/, risorsa che costituisce anche dottrina di riferimento. La figura del *Responsabile de seguridad* viene poi riproposta all'art. 16 della stessa norma: "*El responsable del fichero designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero de acuerdo con este Reglamento.*" Si propone di seguito una traduzione autonoma: "Il responsabile del fascicolo designerà uno o più responsabili della sicurezza preposti al coordinamento e al controllo delle misure definite nel documento di sicurezza. In nessun caso questa designazione implica una delega di responsabilità che corrisponda alla persona responsabile del fascicolo ai sensi del presente regolamento." Si noti qui un elemento caratteristico del responsabile della sicurezza (e di tutte le figure simili come il *privacy officer* e il *data protection officer*): ovvero l'assenza di responsabilità a proprio carico, la quale rimane comunque in capo al responsabile (o titolare, a seconda dei *corpus* normativi) del trattamento.

[136] Cfr. GRECO A., *La nuova figura del data protection officer (Dpo) nell'Ue*, in *Media laws*. *Rivista di Diritto dei Media*, fasc. 1/2021, pp. 305 s.

[137] *First report on the implementation of the Data Protection Directive (95/46/EC) – COM(2003) 265 def.,* Bruxelles, 15 maggio 2003, in https://op.europa.eu/en/publication-detail/-/publication/ff783aa5-5770-42e8-bac3-917fe0a361d7/language-en, p. 27. *Ibidem*.

Capitolo 2: Il nuovo Regolamento: dall'*accountability* al *DPO*

Dopo l'entrata in vigore della Direttiva 95/46/CE, si sono susseguiti altri atti normativi da parte della Comunità Europea (o dell'Unione) in materia di dati personali[1]. Tra questi vi è la Carta di Nizza[2], il cui art. 6, comma 1°: "Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano"[3]. Con il Trattato di Lisbona, il diritto alla protezione dei dati personali viene "costituzionalizzato"[4] all'interno delle tutele dell'Unione europea, diventandone ufficialmente uno dei diritti fondamentali[5].

Una delle conseguenze di questo *upgrade* è la spinta alla Corte di giustizia dell'Unione europea a elaborare una giurisprudenza sempre più incisiva e coraggiosa riguardo sia alle leggi nazionali, sia agli accordi con i paesi terzi[6], sia per quanto riguarda le sentenze ordinarie[7]. Tale processo ha contribuito a formare un voluminoso *corpus* di atti normativi o giurisprudenziali (anche prodotti da organi diversi dalla CGUE, come il WP29) che ha arricchito le regolamentazioni introdotte dalla Direttiva 95/46/CE[8].

In seguito a tali normazioni e decisioni e, come sempre, allo sviluppo tecnologico dei mezzi atti alla gestione

---

[1] Si ricordano qui la *direttiva 2002/58/CE del Parlamento Europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche* e la *direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE*, che non citiamo nel testo per brevità. Ricordiamo però che questi atti sono da intendersi come aggiuntivi e mai sostitutivi della Direttiva 95/46/CE. Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati*, cit., p. 130.

[2] *Carta dei diritti fondamentali dell'Unione Europea*, proclamata a Nizza il 7 dicembre 2000. A seguito del *Trattato di Lisbona che modifica il trattato sull'Unione Europea e il trattato che istituisce la Comunità europea*, firmato il 13 dicembre 2017, la Carta di Nizza ha acquisito il medesimo valore giuridico dei trattati europei (art. 6, *Trattato di Maastricht*, v. nota n. 77, p. 12).

[3] Per completezza riportiamo di seguito anche i commi 2 e 3 del medesimo art.: "*2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.*"

[4] Il termine, utilizzato da PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati*, cit., p. 141, è qui chiaramente improprio, dal momento che l'Unione Europea non dispone di una Costituzione, ma è utile per far capire l'acquisizione, da parte di questo diritto, di uno *status* più importante rispetto al passato (cfr. *ivi*, pp. 140 s.).

[5] Cfr. *ibidem*.

[6] Si pensi ad esempio alla sent. CGUE (Grand Chamber) 6 ottobre 2015, n. C-362/14, in *EUR-Lex*: https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A62014CJ0362, c.d. "sentenza Schrems", con la quale viene invalidato il *Safe Harbor* (Commission Decision 26 July 2000, n. 2000/520/CE, in *EUR-Lex*: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML).

[7] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati*, cit., p. 141.

[8] *Ibidem*.

dei dati personali, è apparsa chiara la volontà della Commissione di dotare l'Unione di un nuovo quadro normativo in materia, il cui protagonista fosse un nuovo regolamento europeo avente come primo obiettivo il raggiungimento di una maggiore conformità tra le varie leggi nazionali, che era stato invece abbandonato durante le trattative che avevano portato alla Direttiva[9].

Per questo motivo il nuovo atto normativo del 27 aprile 2016, n. 679[10] è espresso attraverso lo strumento del regolamento, il quale è per sua natura rivolto non solo agli Stati, ma a tutti i cittadini dell'Unione, essendo direttamente applicabile dal momento dell'entrata in vigore (25 maggio 2018)[11].

Il Regolamento europeo 2016/679 costituisce una svolta epocale[12] nell'ambito della tutela dei dati personali all'interno dell'Unione, introducendo una lunga serie di novità come, tra quelle che riguardano specificamente il nostro percorso, i principi di *accountability*, di *data protection by design & by default*, e la "nuova"[13] figura del *Data Protection Officer*.

2.1 Il principio di *accountability*

Se, come si è detto[14], la Direttiva 95/46/CE era focalizzata sui diritti dell'interessato, nel Regolamento, la tutela dei dati avviene principalmente attraverso la regolamentazione di processi, attività, misure tecniche ed

[9] Cfr. *ivi*, p. 143. V. *supra,* cap. 1, § 1.2.1.

[10] In seguito, "Regolamento" o "*General Data Protection Regulation*" (GDPR).

[11] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati*, cit., p. 150. Come detto, il Regolamento 2016/679/UE (GDPR), non necessita, in prima battuta, di ulteriori atti normativi da parte degli Stati membri. Ciò nonostante, dal momento che il GDPR abroga la precedente Direttiva 95/46/CE (art. 94), ma non le leggi nazionali che la hanno recepita e lascia, talvolta, spazi alla discrezionalità degli Stati, l'entrata in vigore del nuovo Regolamento ha generato una necessità di adeguamento al nuovo *corpus* europeo, che in Italia si è tradotta nel D.Lgs. 10 agosto 2018, n. 101 (c.d. Decreto di adeguamento o Codice novellato), v. PISAPIA A., *La tutela multilivello garantita ai dati personali,* in *Federalismi.it*, n. 3, 31/01/2018, in https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=35666.

[12] Cfr. RICCIO, G. M., SCORZA, G., & BELISARIO, E., *GDPR e normativa privacy. Commentario*, Milano, Wolters Kluwer, 2018, p. 237.

[13] Per una panoramica sui predecessori del *Data Protection Officer*, v. *infra*, cap. 3, § 3.1.

[14] V. *supra*, cap. 1, § 1.2.2.

organizzative, obblighi ed eventuali sanzioni rivolti al titolare[15] del trattamento[16].

Il termine inglese con cui il legislatore si riferisce a tale concetto è "*accountability*", che viene generalmente tradotto in italiano con "responsabilizzazione"[17], anche se non si ritiene che tale traduzione esplichi in modo efficace il concetto nella sua totalità[18].

Il principio è esplicitato all'art. 5 del GDPR[19] dove, dopo aver elencato i "*Principi applicabili al trattamento dei dati personali*"[20], al par. 2° si legge: "*Il titolare del trattamento è competente per il rispetto del paragrafo*

---

[15] Nel GDPR, assume il nome di titolare "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*" art. 4, Regolamento 2016/679/UE. Il titolare è il soggetto che ha in capo la responsabilità giuridica del trattamento.

[16] Cfr. RICCIO, G. M., SCORZA, G., & BELISARIO, E., *GDPR e normativa privacy. Commentario*, Milano, Wolters Kluwer, 2018, p. 237.

[17] La questione della traduzione del termine *accountability* è complessa. Gli stessi RICCIO, G. M & AL., in *GDPR e normativa privacy. Commentario*, Milano, Wolters Kluwer, 2018, p. 237, evidenziano che la traduzione del termine in responsabilizzazione "*necessita di un ulteriore sforzo interpretativo affinché ne venga colto per intero il più ampio* significato".
La traduzione ufficiale indicata dal WP29 in *Opinion 3/2010 on the principle of accountability*, (WP173) 13/07/2010, è "*principio di responsabilità*" (ci si riferisce qui alla prima attestazione del principio all'interno di un atto ufficiale dell'Unione); tale traduzione è stata poi mantenuta nella versione italiana ufficiale del Regolamento. All'interno dello stesso Parere vengono proposte anche una serie di possibili sinonimi e traduzioni del termine *accountability*: "*Nella maggior parte delle altre lingue europee, principalmente a causa delle differenze tra i sistemi giuridici, il termine 'accountability' non è facilmente traducibile […] 'reinforced responsibility' (responsabilità rafforzata), 'assurance' (assicurazione), 'reliability' (affidabilità), 'trustworthiness' (attendibilità) e, in francese, 'obligation de rendre des comptes' (obbligo di rendere conto) ecc. Si potrebbe altresì inferire che 'accountability' si riferisce alla 'attuazione dei principi relativi alla protezione dei dati'*".
In FINOCCHIARO G., *Privacy e protezione dei dati personali: disciplina e strumenti operativi*, Torino, Zanichelli editore, 2016 (I ed. 2012), p. 290, viene proposta la traduzione "*responsabilità e, insieme, prova della responsabilità*". Inoltre, riguardo la traduzione ufficiale del WP29, "*proprio in ragione della complessità del termine e dell'ampiezza dei significati e delle conseguenze cui può riferirsi, si ritiene preferibile continuare ad utilizzare il termine originario 'accountability', invece che la traduzione «principio di responsabilità»*", *ibidem.*
Infine, BOLOGNINI L., PELINO E. & BISTOLFI C. optano per la traduzione in "responsabilizzazione", in *Il regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, Giuffrè, 2016, pp. 323 ss.

[18] "*Quello di accountability è un concetto difficilmente traducibile in una parola della nostra lingua e reso, nella versione italiana del regolamento, con il termine "responsabilità". In realtà, esso si colloca a metà tra la responsabilità e la compliance, perché il titolare deve essere compliant rispetto alla normativa in esame. Bisognerà trovare un termine diverso o composto per evitare l'utilizzo del termine "responsabilità": problemi di traduzione esistono, ogni lingua ha dei termini difficilmente traducibili e quello dell'accountability appare proprio uno di questi casi.*" LUCCHINI GUASTALLA E., *Il nuovo Regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contratto e Impresa*, vol. 34, n. 1, 2018, pp. 106 - 125, in https://studiolegale.leggiditalia.it/#id=10AR0000189258ART1,__m=document.

[19] Anche se il concetto di *accountability* viene esplicitamente citato all'art. 5 e poi definito all'art. 24, esso è presente nell'intero *corpus* della nuova normativa, della quale costituisce il cardine dell'approccio basato sulla gestione del rischio. Cfr. FINOCCHIARO G., *GDPR tra novità e discontinuità: il principio di accountability*, in *Giurisprudenza Italiana*, vol. 12, 2019, p. 2777 ss.

[20] Rubrica art. 5, Regolamento 2016/679/UE.

1 e in grado di comprovarlo (responsabilizzazione)"[21]. All'*accountability* è poi dedicato l'intero art. 24: "*Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravita 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. Dette misure sono riesaminate e aggiornate qualora necessario*"[22].

Secondo il Considerando n. 74 del Reg.[23], l'*accountability* combina due aspetti: in primo luogo l'adozione da parte del titolare di "*misure adeguate ed efficaci*" per garantire che il trattamento dei dati sia effettuato in modo conforme al Regolamento e, in seconda battuta, il fatto che egli sia in grado di dimostrare l'adeguatezza delle misure realizzate in virtù dell'art. 24[24].

Si tratta di un notevole cambio di paradigma nella tutela dei dati personali: non sono più previste soltanto una serie di prescrizioni dirette da seguire per non incorrere in una sanzione, ma viene posto un obiettivo che il titolare deve perseguire determinando egli stesso le modalità adeguate di volta in volta[25]. A questo proposito, i già citati Riccio, Scorza e Belisario hanno definito l'introduzione dell'*accountability* come "*un vero e proprio cambiamento culturale*" che incoraggia chi tratta dati personali a "*cambiare 'mentalità' e ad essere responsabili e pro-attivi, sin dalla prima fase del trattamento dei dati*"[26].

---

[21] Per questa citazione dal Regolamento 2016/679/UE e per tutte quelle in seguito, si è utilizzato il testo ufficiale pubblicato sul sito del Garante per la protezione dei dati personali, in https://www.garanteprivacy.it/il-testo-del-regolamento.

[22] Si riportano di seguito i par. 2 e 3 dello stesso art.: "*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. 3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento*".
Per comprendere appieno il significato di tale art., è opportuno riportare anche il Considerando n. 74 (c74): "*È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. 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.*"

[23] Si riferiscono al Regolamento anche tutti i Considerando citati in seguito.

[24] Cfr. BOLOGNINI L. & AL., *Il regolamento privacy europeo: commentario*, cit., pp. 324 s.

[25] Cfr. FINOCCHIARO G., *GDPR tra novità e discontinuità: il principio di accountability*, in *Giurisprudenza Italiana*, vol. 12, 2019, p. 2777 ss.

[26] RICCIO, G. M., SCORZA, G., & BELISARIO, E., *GDPR e normativa privacy*, cit., pp. 237 s.

Si può dire, in tal senso, che l'*accountability* costituisca una sorta di "principio dei principi"; ciò è ribadito anche attraverso l'art. 30 del Regolamento, il quale obbliga il titolare (o il responsabile da questi indicato) a tenere un "*Registro delle attività di trattamento*"[27]: uno degli elementi imprescindibili per dimostrare il rispetto del principio di *accountability*[28].

L'introduzione dell'*accountability* risponde alle criticità individuate dal WP29 rispetto al quadro normativo antecedente al Regolamento: "[si ritiene che] *l'attuale quadro giuridico non sia riuscito appieno a garantire che gli obblighi in materia di protezione dei dati si traducano in meccanismi efficaci atti a fornire una protezione reale*"[29] si legge all'interno del già citato *Parere 3/2010 sul principio di responsabilità*. Secondo lo stesso documento, l'eventuale introduzione di un principio di responsabilizzazione avrebbe contribuito "*a passare 'dalla teoria alla pratica' e ad aiutare le autorità di protezione dei dati nello svolgimento dei loro compiti di controllo e di verifica*"[30].

2.1.1 Origine storica

Non è semplice determinare il periodo storico in cui il concetto di *accountability* è stato applicato per la prima volta, soprattutto perché tale concetto è utilizzato in discipline diverse.

Secondo Mahomoud Ezzamel le radici del concetto di *accountability* in ambito economico affondano nell'antico Egitto, nel c.d. Nuovo Regno (1552 – 1069 a.C.), all'interno di un sistema evoluto di ridistribuzione dei beni, coordinato da un'accurata burocrazia fondata, appunto, su un sistema di rendicontazione[31]. Esempi

---

[27] Rubrica art. 30, Regolamento 2016/679/UE.

[28] Cfr. BOLOGNINI L., PELINO E. & BISTOLFI C., *Il regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, Giuffrè, 2016, pp. 324 s.

[29] Article 29 Working Party, *Opinion 3/2010 on the principle of accountability*, WP173, Bruxelles, 13/07/2010, in https://www.garanteprivacy.it/documents/10160/10704/Articolo+29+-+WP173+-+Parere+3+2010+sul+principio+di+responsabilit%C3%A0.pdf/006f43b3-7180-4485-903e-bf8b4f367763?version=1.2, p. 3.

[30] *Ivi*, p. 2.

[31] V. EZZAMEL M., *Accounting, control and accountability: preliminary evidence from ancient Egypt*, in *Critical perspective on accounting*, Manchester University academic press, vol. 8, 1997, pp. 563 – 601, in https://www.sciencedirect.com/sdfe/reader/pii/S1045235497901234/pdf, si riporta di seguito la versione in lingua originale: "*Drawing on evidence from the New Kingdom 1552 ( )]1069 BC in ancient Egypt, this paper provides some preliminary findings relating to the functioning of accounting particularly as it relates to control and accountability. Ancient Egypt evolved a redistributive economic system which remained prevalent for most of her long history. The political and economic domains were coordinated by a powerful bureaucracy in which accounting played a major role. The evidence suggests that the intervention of accounting was manifest in many ways, in particular defining and constituting the domain of economic activities, and through measurement and quantification accounting imparted visibility and with it particular meanings and significance upon such activities. Examples of accounting's intervention include the quantification of input-output relationships, such as in the case of baking bread or brewing beer, and the*

di questo sistema sono i reperti che riportano elenchi di risorse e materiali, come antenati del pane o della birra, costruiti secondo una logica input-output, che evidenziasse il corretto comportamento del singolo rispetto alla comunità[32].

Altri studi individuano le radici di quello che sembra sempre più un "principio dei principi"[33] in altre civiltà come la Cina imperiale, la Mesopotamia, Israele, e l'antica Grecia[34], ma Melvin J. Dubnick ha tracciato una sorta di linea ideale tra il concetto da lui stesso definito "primitivo"[35] di *accountability* e la nascita del concetto "contemporaneo"[36], ponendola tra il X e il XII secolo d.C.

Dubnick parte dall'analisi dell'etimologia delle parole con cui le varie lingue europee si riferiscono a questo concetto e nota come l'inglese si distingua dalle lingue romanze (portoghese, italiano, francese, spagnolo), le quali utilizzano varie forme del termine "*responsability*" in sostituzione del termine inglese "*accountability*"[37]. *Accountability* non è però un sinonimo di *responsability*, come ricorda anche John Uhr[38]; al massimo ne è complementare e comunque non uguale.

Ciò che invece si avvicina di più ad una corretta traduzione di "*accountability*" è una frase descrittiva che nella nostra lingua possiamo rendere con "l'atto di rendere conto"[39]. Più precisamente, il termine "*accountability*" indica l'idea di rendere conto di qualcosa a qualcuno in un contesto istituzionale, ma mentre in altre lingue, come l'italiano, è necessaria una frase più complessa per esprimere il concetto, in inglese questo è espresso con un singolo lemma. Per questo motivo l'*accountability* viene oggi definito come un concetto di origine

---

construction of lists of inventories in the palace, the temples, and the royal granaries. Measures used were expressed in physical terms and the accounting practices which emerged were sufficiently developed to operate as systems of accountability even though there is no direct evidence to confirm that they were used as such".

[32] *Ibidem*.

[33] V. *supra*, cap. 2, § 2.1.

[34]Cfr. DUBNICK M. J., *Accountability as Cultural Keyword*, in *Oxford Handbook of Public Accountability*, Oxford, Oxford Univrsity Press, 2014, pp. 23 – 38, in http://mjdubnick.dubnick.net/papers/2012/Dubnick%20VU%202012.pdf.

[35] Eng. *primitive, ibidem*.

[36] Eng. *today's accountability*, *ibidem*.

[37]Cfr. DUBNICK M. J., *Clarifying Accountability: An Ethical Theory Framework*, in *Public Sector Ethics Finding and Implementing Value*s, Sydney, Federation Press, 1998, chapter 5, pp. 68 - 81, in http://mjdubnick.dubnick.net/pubsrw/1998/dub1998clar.html.

[38]Cfr. UHR J., *Redesigning Accountability: From Muddles to Maps*, in The Australian Quarterly, vol. 65, n. 2, pp. 1 - 16, in https://www.jstor.org/stable/pdf/20635716.pdf.

[39] La traduzione in italiano è di chi scrive. Dubnick propone l'eng. "*the rendering of accounts*" e il fr. "c*omptes a rendre*" (DUBNICK M. J., *Clarifying Accountability: An Ethical Theory Framework*, cit., p. 70).

anglosassone[40].

Proseguendo nella sua ricostruzione storica, lo stesso studioso indica come evento spartiacque, nell'evoluzione storica dell'*accountability,* la pubblicazione del Manoscritto di Doomsday[41] nel 1086[42]. Vent'anni dopo la conquista normanna dell'Inghilterra[43], William I[44] ordinò un censimento generale di tutti possedimenti terrieri dello Stato, opera che fu completata in circa due anni e viene oggi considerata come una tappa fondamentale del consolidamento del potere centralizzato nella terra di Shakespeare[45]. Lo scopo dell'indagine non era solo di natura tributaria, ma anche la manifestazione della nuova sovranità normanna: poco dopo, infatti, i proprietari terrieri furono chiamati a giurare fedeltà alla corona e fu istituito un sistema di controllo semestrale, basato sulla rendicontazione di questi nei termini stabili dagli incaricati al controllo[46].

È qui necessaria una precisazione: ovvero il fatto che nel XI secolo i possedimenti su suolo inglese appartenevano solo parzialmente ai proprietari: infatti in questo tipo di regimi ogni appezzamento di terreno era formalmente di proprietà del sovrano[47]. In quest'ottica, lo scenario illustrato da Dubnick assume, agli occhi di chi scrive, un significato diverso: si tratta di un soggetto, il Re in questo caso, che cede ad altri, i proprietari, l'utilizzo di beni che gli appartengono e che producono ricchezza economica, le terre, sui quali mantiene però un controllo attraverso un sistema di rendicontazione basato su principi da lui stesso istituiti, ma che vengono verificati *ex-post* rispetto allo sfruttamento dei suddetti beni.

Ora si pensi al modello di gestione del rischio introdotto dal GDPR: l'interessato cede al titolare del trattamento il diritto all'utilizzo dei dati che, come abbiamo detto[48], sono beni in grado di produrre valore economico, mantenendo su di essi un controllo attraverso il sistema di *accountability* (art. 24, Regolamento 2016/679/UE)

---

[40] Cfr. *ivi*, pp. 70 ss.

[41] Eng. *Doomsday Books*.

[42] Cfr. DUBNICK M. J., *Clarifying Accountability: An Ethical Theory Framework*, cit., pp. 70 s.

[43] Ci si riferisce all'invasione e l'occupazione di una parte della Gran Bretagna da parte di un esercito di soldati normanni, bretoni e francesi, guidati da William I, detto "il conquistatore" culminata con la vittoria degli invasori nella battaglia di Hastings del 14 ottobre 1066.

[44] Il cui nome è stato, in seguito alla fastidiosa pratica di italianizzare i nomi stranieri, tradotto nei libri di storia in Guglielmo I.

[45] Cfr. DUBNICK M. J., *Clarifying Accountability: An Ethical Theory Framework*, cit., pp. 70 s.

[46] *Ibidem*.

[47] Cfr. BANTI A. M., *L'età contemporanea. Dalle rivoluzioni settecentesche all'imperialismo*, Bari, Laterza, 2009, p. 108.

[48] V. nota n. 28, p. 6.

basato sui principi stabiliti all'art. 5. Sotto questo punto di vista, i due modelli sembrano, con le dovute differenze dovute all'epoca storica, alle caratteristiche dei soggetti e dei beni in questione, sovrapponibili.

2.1.2 Adeguatezza ed efficacia delle misure

L'art. 24 del GDPR definisce "*adeguate*" le misure che il titolare (o un suo delegato) deve adottare al fine di rispettare i principi generali del trattamento (espressi all'art. 5). È importante sottolineare che il concetto di adeguatezza si riferisce ad una verifica *antecedente* alla messa in atto del trattamento, come da combinato disposto dell'art. 24.1 e del c74[49].

Il fatto che gli articoli e il Considerando citati non contengano un elenco di misure ritenute adeguate per definizione ribadisce che il titolare debba effettuare una valutazione caso per caso, in conseguenza "*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*"[50]. Ciò non deve apparire come un passo indietro rispetto alle dettagliate misure previste nella Direttiva 95/46/CE o nel Codice privacy italiano[51], ma come un'ulteriore riaffermazione della nuova gestione del rischio proposta dal Regolamento[52].

Una parte della dottrina ha visto nell'assenza, almeno fino a questo punto, di misure[53] indicate, la volontà del legislatore di garantire la scalabilità della protezione dei dati in contesti anche estremamente differenti tra loro. Si precisa tuttavia che all'interno del GDPR sono prescritte misure obbligatorie in determinati casi, la cui adozione assicura il rispetto dell'*accountability*[54], come ad esempio la nomina di un DPO; la presenza di tali misure non va però ad inficiare la *ratio* sottesa all'impostazione generale del Regolamento.

La valutazione *ex ante* non esaurisce però l'essenza del principio di responsabilizzazione, il quale si completa invece con una verifica *ex post* dell'*efficacia* delle misure adottate[55].

Su come assicurare l'efficacia delle misure si è espresso il WP29 nel già citato Parere 3/2010: "*Per il*

---

[49] Cfr. RICCIO, G. M., SCORZA, G., & BELISARIO, E., *GDPR e normativa privacy*, cit., pp. 235 s.

[50] C74, Regolamento 2016/679/UE.

[51] Si pensi alle misure minime di sicurezza previste all'All. B, d.lgs. 30 giugno 2003, n. 196, rubricato "*Disciplinare tecnico in materia di misure minime di sicurezza*".

[52] Cfr. BOLOGNINI L. & AL., *Il regolamento privacy europeo: commentario*, cit., p. 326.

[53] V. *ibidem* e FINOCCHIARO G., *GDPR tra novità e discontinuità*, cit., pp. 2777 ss.

[54] Cfr. BOLOGNINI L. & AL., *Il regolamento privacy europeo: commentario*, cit., p. 326.

[55] L'art. 24, Regolamento 2016/679/UE definisce le misure da mettere in atto come "*adeguate*" ed "*efficaci*".

trattamento di dati di maggiori dimensioni, più complesso e ad alto rischio, gli audit interni ed esterni sono metodi comuni di verifica […] *Nel decidere come garantire l'efficacia delle misure, il Gruppo di lavoro articolo 29 suggerisce di utilizzare gli stessi criteri applicati per decidere le misure mutuati dall'articolo 17 della direttiva 95/46/CE, vale a dire, i rischi presentati dal trattamento e la natura dei dati. Pertanto, il modo in cui un responsabile* [titolare, nda][56] *del trattamento deve assicurare l'efficacia delle misure dipende dalla sensibilità dei dati, dalla quantità dei dati trattati e dai particolari rischi che il trattamento comporta*"[57].

La responsabilità del titolare non è dunque limitata al porre in essere delle misure adeguate, ma si estende anche alla puntuale e sistematica verifica della loro efficacia; inoltre, le verifiche appena descritte devono essere non solo eseguite, ma anche documentate, al fine di provare all'autorità di controllo la conformità ai principi espressi all'art. 5[58]. "*L'accountability passa per le modalità in cui viene esercitata la responsabilità (adozione di misure adeguate), ma anche attraverso la verificabilità della responsabilità stessa (efficacia delle misure adottate)*"[59].

2.1.3 I due livelli di *accountability*: obblighi e iniziative

In generale, l'*accountability* è un meccanismo a due livelli[60], il primo dei quali è costituito da obblighi di base vincolanti per tutti i titolari di trattamento; tali obblighi comprendono due elementi fondamentali: l'attuazione di misure tecniche e organizzative in conformità ai principi espressi all'art. 5 del GDPR e, come abbiamo detto, la conservazione delle prove di tale attuazione[61].

Il secondo livello è invece costituito da *iniziative* di natura volontaria, che il titolare mette in atto in virtù dei principi fondamentali di protezione dei dati. Tali iniziative eccedono i requisiti minimi di conformità al Regolamento e includono garanzie più elevate e/o termini di attuazione più specifici[62]. Una delle iniziative

---

[56] Si ricorda che questo Parere è stato pubblicato quando era ancora in vigore la Direttiva 95/46/CE, di cui utilizza la terminologia.

[57] Article 29 Working Party, *Opinion 3/2010 on the principle of accountability*, WP173, Bruxelles, 13/07/2010, p. 16.

[58] Cfr. BOLOGNINI L. & AL., *Il regolamento privacy europeo: commentario*, cit., p. 327.

[59] *Ibidem*.

[60] Cfr. FINOCCHIARO G., *Privacy e protezione dei dati personali: disciplina e strumenti operativi*, cit., pp. 290 s.

[61] *Ibidem*. Cfr. anche Article 29 Working Party, *Opinion 3/2010 on the principle of accountability*, WP173, Bruxelles, 13/07/2010, p. 6.

[62] *Ibidem* (entrambi).

volontarie tipiche del secondo livello è la nomina di un *Data Protection Officer* quand'anche non sia specificamente prescritto dalla normativa vigente, come suggerito dal WP29[63].

Alla luce di questi due livelli, l'*accountability* può essere vista come un metodo per formalizzare l'autonomia concessa nei limiti del Regolamento: sostanzialmente un modo, di radici anglosassoni[64], per compensare autonomia e procedure[65]. In questo caso, risulta chiaro che la valenza dell'*accountability* muta notevolmente al variare del grado di autonomia che viene concesso al titolare dalla normativa vigente[66].

A questo proposito, i più entusiasti hanno visto l'*accountability* "*non* [...] *solo come un principio fonte di obblighi per il titolare, ma* [...] [come] *una felice prassi adottata da tutti i titolari nel porre in essere attività di trattamento di dati personali*"[67].

Un'altra lettura può essere legata al fatto che, nonostante la motivazione alla base dell'introduzione dell'*accountability* sia migliorare l'attuazione pratica del diritto, viene lasciato spazio anche ad una certa adattabilità del diritto stesso, che consenta di applicare il medesimo Regolamento ad una serie di situazioni mutevoli, eterogenee e in continua evoluzione, proprio laddove la Direttiva 95/46/CE non era riuscita a spingersi[68].

---

[63] Article 29 Working Party, *Linee-guida sui responsabili della protezione dei dati (RPD)*, WP243 rev. 1, Bruxelles, 13/12/2016, versione emendata e adottata 05/04/ 2017, in https://www.cyberlaws.it/wp-content/uploads/2017/07/Linee-guida-sui-responsabili-della-protezione-dei-dati-RPD-WP-243.pdf, p. 3.

[64] V. *supra*, cap. 2, § 2.1.1.

[65] Cfr. FINOCCHIARO G., *Privacy e protezione dei dati personali: disciplina e strumenti operativi*, cit., p. 291.

[66] *Ibidem*.

[67] Cfr. RICCIO, G. M. & AL., *GDPR e normativa privacy*, cit., p. 244.

[68] Cfr. BOLOGNINI L. & AL., *Il regolamento privacy europeo: commentario*, cit., pp. 333 s. Cfr. anche RICCIO, G. M. & AL., *GDPR e normativa privacy*, cit., p. 238.

2.2 *Data protection by design*

Il principio di *data protection by design*, o *privacy by design* (*PBD*), è uno dei principi che derivano dall'*accountability*[69] e riguarda la "*protezione dei dati fin dalla progettazione*"[70].

2.2.1 Prima del Regolamento

Il concetto di *privacy by design* è legato al nome di Ann Cavoukian, *Information and Privacy Commissioner* dell'Ontario dal 1997 al 2014, che negli anni '90 ne teorizzò i concetti base, articolandoli in sette principi fondamentali[71].

1. Proattività, non reattività; agire in modo preventivo e non in correzione[72].
2. Privacy come impostazione di default[73].
3. Privacy incorporata nella progettazione[74].
4. Massima funzionalità; valore positivo, non somma zero[75].
5. Protezione dall'inizio alla fine; protezione durante tutto il ciclo-vita[76].

---

[69] Cfr. BOLOGNINI L. & AL., *Il regolamento privacy europeo: commentario*, cit., p. 340. Inoltre, il legame tra *accountability* e *data protection by design* (e *by default*) è sottolineato anche dall'art. 82, comma 2.d, che prevede che, nel decidere riguardo all'eventualità e all'importo di una sanzione amministrativa, si debba tener conto del "*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*".

[70] Rubrica art. 25, Regolamento 2016/679/UE.

[71] Cfr. RICCIO, G. M. & AL., *GDPR e normativa privacy*, cit., p. 248.

[72] L'approccio *PBD* è caratterizzato da misure proattive in sostituzione di quelle reattive; previene l'invasione della privacy prima che questa avvenga, in sostanza: la *PBD* agisce *ex ante*, non *ex post.* Cfr. CAVOUKIAN A., *Privacy by Design. The 7 Foundational Principles*, in *privacybydesign.ca*, *Information of Privacy Commissioner of Ontario*, 05/2010, rev. 01/2011, in https://privacysecurityacademy.com/wp-content/uploads/2020/08/PbD-Principles-and-Mapping.pdf, p. 2.

[73] V. *infra*, cap. 2, § 2.2.3.

[74] La *PBD* è integrata nelle caratteristiche e nell'architettura dei sistemi IT e nel *business plan*, non è aggiunta *ex post* come un corpo esterno. Il risultato è che la privacy sia una componente fondamentale delle funzionalità *core* del prodotto: il rispetto della privacy è integrato nel sistema, senza ridurne la funzionalità. Cfr. CAVOUKIAN A., *Privacy by Design. The 7 Foundational Principles*, cit., p. 3.

[75] L'approccio *PBD* cerca di soddisfare tutti gli interessi e gli obiettivi in un rapporto *win-win*, senza ricorrere ad un anacronistico approccio "a somma zero", dove trovano spazio inutili compromessi. (eng. "*a dated, zero sum approach, where unnecessary trade-offs are made*", trad. autonoma). La *PBD* evita il pretesto delle false dicotomie, come *privacy vs. security*, dimostrando che è possibile, e ancor meglio auspicabile, averle entrambe. Cfr. CAVOUKIAN A., *Privacy by Design. The 7 Foundational Principles*, cit., pp. 3 s.

[76] Essendo stata incorporata nel sistema prima dell'avvio del trattamento, la *PBD* si estende lungo tutto il ciclo-vita dei dati trattati: sono necessarie misure di sicurezza forti fin dall'inizio alla fine del trattamento. Ciò significa che tutti i dati raccolti sono conservati in sicurezza e vengono cancellati in modo definitivo alle fine del processo. Cfr. CAVOUKIAN A., *Privacy by Design. The 7 Foundational Principles*, cit., p. 4.

6. Visibilità e trasparenza[77].
7. Rispetto per la privacy dell'utente; centralità dell'interessato[78].

Gli stessi principi sono stati oggetto di discussione durante la XXXII Conferenza mondiali dei Garanti per la protezione dei dati personali, tenutasi a Gerusalemme nel 2010, in seguito alla quale è stato pubblicato un documento[79] che sostanzialmente ribadisce i sette principi teorizzati da Cavoukian[80].

Un'altra definizione di *privacy by design* antecedente al Regolamento è quella di Demetrius Klitou: la realizzazione dei valori, in questo caso i principi della privacy e norme/regolamenti corrispondenti, tramite la progettazione fisica, le specifiche tecniche, l'architettura e/o il codice informatico del dispositivo, sistema, tecnologia o servizio in questione, ove applicabile[81].

Per lo stesso autore, il significato della *protection by design* è che il rispetto dei principi di liceità del trattamento sia uno degli obiettivi primari nel corso della progettazione di un prodotto, un servizio o un software, rendendo così l'output *privacy-friendly* per sua stessa natura[82].

Lo stesso autore si riferisce di nuovo alla *privacy by design* in termini di misure pratiche, sotto forma di soluzioni tecnologiche e di progettazione, mirate a rafforzare l'applicazione delle leggi sulla protezione dei

---

[77] L'approccio *PBD* assicura a tutte le parti interessate che, qualunque sia la pratica commerciale o tecnologica coinvolta, questa avvenga secondo le premesse e gli obiettivi dichiarati, essendo poi soggetta a verifica da parte di un'Autorità indipendente. Tutte le componenti e i processi sono visibili e trasparenti, sia per gli utenti, sia per i fornitori. Cfr. CAVOUKIAN A., *Privacy by Design. The 7 Foundational Principles*, cit., pp. 4 s.

[78] L'approccio *PBD* richiede ai progettisti e agli operatori (la trad. è qui autonoma e letterale; eng. "*architects and operators*", ma proponiamo anche la versione, più in linea con il GDPR: "ai titolari e a tutti gli incaricati") di attribuire la massima priorità agli interessi dell'utente, garantendo misure di *privacy by default* (v. *infra*, cap. 2, § 2.2.3) un'informativa adeguata e soluzioni *user-friendly*. Cfr. CAVOUKIAN A., *Privacy by Design. The 7 Foundational Principles*, cit., p. 5.

[79] 32nd International Conference of Data Protection and Privacy Commissioners, *Resolution on Privacy by Design*, Jerusalem, 27-29 October 2010, in https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1807346.

[80] Cfr. RICCIO, G. M. & AL., *GDPR e normativa privacy*, cit., p. 249.

[81] La traduzione è autonoma, eng. "*The realization of values, in this case the principles of privacy and corresponding rules/regulations, via the physical design, technical specifications, architecture and/or computer code of the device, system or technology concerned, where applicable*", in KLITOU D., *Privacy-Invading Technologies and Privacy by Design*, The Hague, TMC Asser Press, 2014, in https://link.springer.com/content/pdf/10.1007%2F978-94-6265-026-8.pdf, p. 262.

[82] Cfr. KLITOU D., *Privacy-Invading Technologies and Privacy by Design*, cit., pp. 262 ss.

dati, o meglio a garantire la conformità alle stesse e riducendo al minimo le capacità intrusive della privacy da parte delle tecnologie interessate[83].

2.2.2 Nel Regolamento

Il Regolamento dedica all'approccio *privacy by design* l'art. 25, il quale si apre con uno sguardo d'insieme su tutti i fattori che il titolare deve tenere in considerazione nello svolgere il suo ruolo; questa panoramica, i cui elementi, si ricorda, sono esemplificativi e non esaustivi, consentirà al titolare di assicurarsi che i trattamenti intrapresi, o che sta per intraprendere, non violino il Regolamento[84].

Così, il titolare deve interessarsi "*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*"[85]. A chi determina i trattamenti è quindi richiesto di agire con ponderazione e flessibilità, continuando a perseguire l'obiettivo primario di rispetto della normativa e dei diritti degli interessati[86].

L'art. 25 integra quindi l'art. 24, di cui riprende parte del testo, individuando il frangente temporale in cui bisogna adempiere a quanto già espresso nell'art. precedente sia nel momento in cui il trattamento è già operativo, ma soprattutto nelle fasi preliminari alla messa in atto dello stesso[87].

Venendo ora al c78, questo approccio dovrebbe essere adottato "*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*"[88]. Per fare in modo che ciò avvenga, anche 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*

---

[83] La traduzione è autonoma, eng. "*In other words, PBD can be defined as practical measures, in the form of technological and design-based solutions, aimed at bolstering privacy/data protection laws, better ensuring or almost guaranteeing compliance, and minimizing the privacy-intrusive capabilities of the technologies concerned*". *Ivi*, pp. 262 s.

[84] Cfr. RICCIO, G. M. & AL., *GDPR e normativa privacy*, cit., p. 247.

[85] Art. 25, par. 1°, Regolamento 2016/679/UE.

[86] Cfr. RICCIO, G. M. & AL., *GDPR e normativa privacy*, cit., p. 247.

[87] *Ibidem.*

[88] C78, Regolamento 2016/679/UE.

dei dati"[89].

In prima battuta, lo scopo della *privacy by design* nel Regolamento è assicurare che le garanzie di protezione dei dati personali non siano trascurate né in fase di progettazione iniziale dei trattamenti, né nei loro successivi funzionamenti e sviluppi[90], ponendo particolare attenzione al fatto che procedimenti e modalità di trattamento siano strutturalmente coerenti con i vincoli della normativa perché costruiti, fin dalla fase iniziale, in funzione delle tipologie di dati trattati e delle finalità perseguite[91].

Questo tipo di regolazione si caratterizza per la scalabilità nella sua applicazione, rendendosi molto più adatto, rispetto ad esempio alla Direttiva 95/46/CE, alla varietà di situazioni eterogenee che caratterizzano il mondo digitale contemporaneo[92].

Se l'approccio *privacy by design* è precedente al Regolamento, quest'ultimo introduce una nuova specifica modalità di implementazione: ovvero il fatto che le misure ex art. 25 abbiano il duplice obiettivo di applicare i principi ex art. 5, ma anche di integrare nel trattamento le relative garanzie[93]. In sostanza la tutela deve essere implementata *attraverso* il trattamento e *come effetto* del trattamento stesso; questa nuova finalità si aggiunge a quella personale perseguita dal titolare, con la quale si sviluppa secondo il quarto principio della *PBD* di Cavoukian[94]. La conseguenza di questo approccio innovativo è che la tutela divenga parte integrante del trattamento in sé considerato[95].

Anche in questo caso non vengono prescritte soluzioni tecniche o organizzative specifiche[96], ma la normativa si limita a ribadire i principi: questo è espressione della neutralità del principio di *data protection-by-design*[97]. Ciò consente ai titolari, ai responsabili, agli eventuali *Data Protection Officer* e alle Autorità nazionali, di interpretare il significato del principio in ogni caso specifico. La valutazione caso per caso si colloca

---

[89] *Ibidem*.

[90] Cfr. RICCIO, G. M. & AL., *GDPR e normativa privacy*, cit., p. 247.

[91] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati*, cit., p. 287.

[92] *Ibidem.*

[93] Cfr. RICCIO, G. M. & AL., *GDPR e normativa privacy*, cit., p. 249.

[94] *Ibidem*.

[95] *Ibidem.*

[96] Eccezion fatta per la pseudonimizzazione.

[97] Cfr. BOLOGNINI L. & AL., *Il regolamento privacy europeo: commentario*, cit., p. 342.

perfettamente sulla linea tracciata dall'art. 24 che, come abbiamo visto[98] , non indica misure adeguate in ogni situazione, ma lascia ampia indipendenza riguardo all'adozione delle dette misure, ricordando che la responsabilità del titolare dipende dai fattori che abbiamo elencato poco sopra[99].

Tuttavia, il GDPR non lascia il titolare totalmente sprovvisto di una guida: infatti, il c28[100], gli art. 4, par. 5[101] (in cui ne compare la definizione) e l'art. 25[102], introducono la misura della pseudonimizzazione[103]. Inoltre, il già citato art. 25 introduce nel quadro normativo europeo un altro principio di grande rilievo nello sviluppo dell'*accountability*, un principio che è sempre stato legato all'approccio *protection by design* fin dall'iniziale elaborazione di Cavoukian: la minimizzazione.

2.2.3 Minimizzazione e *data protection by default*

Il concetto di *data protection by default*, o *privacy by default*[104], viene definito da Cavoukian come uno dei sette principi dell'approccio *privacy by design*[105]; a differenza degli altri però, questo principio non riguarda la fase di trattamento dei dati, bensì quella di raccolta.

Secondo Cavoukian, la *privacy by default* si concretizza quando i dati sono *automaticamente* protetti in qualsiasi sistema informatico o azienda: ovvero, se l'utente non modifica le opzioni di trattamento, la sua privacy non subisce lesioni (salvo quando sia strettamente necessario). Non è cioè necessaria alcuna azione da

---

[98] V. *supra*, cap. 2, § 2.1.3.

[99] Cfr. BOLOGNINI L. & AL., *Il regolamento privacy europeo: commentario*, cit., p. 342.

[100] "*L'applicazione della pseudonimizzazione ai dati personali può ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati. L'introduzione esplicita della «pseudonimizzazione» nel presente regolamento non è quindi intesa a precludere altre misure di protezione dei dati*". Si ricorda che il tema della pseudonimizzazione è trattato anche nei c26 e c29, che non riportiamo per brevità.

[101] "*«pseudonimizzazione»: 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.*"

[102] "[...] *misure tecniche e organizzative adeguate, quali la pseudonimizzazione* [...]".

[103] Cfr. RICCIO, G. M. & AL., *GDPR e normativa privacy*, cit., p. 249. Si ricorda che la misura di pseudonimizzazione è diversa dall'anonimizzazione, la quale segna il confine che determina la riconducibilità di un trattamento all'interno dell'ambito di applicazione del Regolamento. Infatti, come espresso nel C26: "*I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca.*"

[104] It. protezione dei dati per impostazione predefinita.

[105] V. *supra,* cap. 2, § 2.2.1.

parte dell'interessato per proteggere la sua stessa privacy, in quanto la tutela è integrata nel sistema per impostazione predefinita[106].

Nello stesso documento, Cavoukian individua delle buone pratiche[107] con cui il principio di *privacy by default* deve essere implementato, tra le quali troviamo la "*Data Minimization*"[108] o minimizzazione, secondo cui la raccolta di dati personali deve essere limitata alle informazioni strettamente necessarie.

Secondo la *data minimization*, la progettazione dei programmi, dei dispositivi di informazione e comunicazione e dei sistemi dovrebbe iniziare con interazioni e transazioni non identificabili come impostazione predefinita; inoltre, ovunque sia possibile, l'identificabilità, l'osservabilità e la possibilità di collegare le informazioni all'interessato dovrebbero essere ridotte al minimo[109].

All'interno del Regolamento, invece, il rapporto tra *data protection by default* e *minimization* è ribaltato. Il principio di minimizzazione (art. 5, par. 1c[110] e art. 25[111]) non è visto come una misura pratica derivante dall'approccio *privacy by default*, ma ne costituisce il presupposto[112].

La *privacy by default* rappresenta quindi, nel quadro europeo, una forma di applicazione concreta del principio di minimizzazione, volta, nell'ambito di una tecnologia o di un processo, a raccogliere ed elaborare solo i dati personali strettamente necessari per consentire l'erogazione del servizio richiesto dall'interessato, assicurandogli un trattamento legittimo per impostazione predefinita[113].

---

[106] Cfr. CAVOUKIAN A., *Privacy by Design. The 7 Foundational Principles*, cit., pp. 2 s.

[107] Eng. "*Fair Information Practices*", trad. autonoma. *Ibidem*.

[108] V. CAVOUKIAN A., *Privacy by Design. The 7 Foundational Principles,* cit., p. 3.

[109] Eng. "*The collection of personally identifiable information should be kept to a strict minimum. The design of programs, information and communications technologies, and systems should begin with non-identifiable interactions and transactions, as the default. Wherever possible, identifiability, observability, and linkability of personal information should be minimized*". *Ibidem*, trad. autonoma.

[110] "*I dati personali sono* [...] *adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»)*".

[111] "[...] *misure tecniche e organizzative adeguate* [...] *volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione*".

[112] Cfr. BOLOGNINI L. & AL., *Il regolamento privacy europeo: commentario*, cit., p. 108.

[113] *Ibidem*. L'*European Data Protection Board* ha proposto il seguente esempio all'interno delle *Linee guida 4/2019 sull'articolo 25. Protezione dei dati fin dalla progettazione e per impostazione predefinita*, versione 2.0, 20 ottobre 2020, in https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_it.pdf, p. 23: "*Una libreria intende aumentare le entrate vendendo i libri online. Il proprietario vuole creare un modello standardizzato per il procedimento di ordinazione. Per garantire che i clienti forniscano tutte le informazioni richieste, il proprietario della libreria rende obbligatori tutti i campi del modulo (se non si compilano tutti i campi il cliente non può effettuare l'ordine). Inizialmente, il proprietario del negozio online usa un modulo di contatto standard in cui si chiedono al cliente informazioni quali la data di nascita, il numero di telefono e l'indirizzo di casa. Tuttavia, i*

Bisogna sottolineare che il principio di minimizzazione va interpretato, nel contesto del Regolamento, sia in dimensione quantitativa, sia in dimensione qualitativa[114]. Quanto alla prima, l'effetto del principio è evidente, dal momento che impone lo svolgimento del trattamento esclusivamente nella misura indispensabile all'erogazione del servizio richiesto dall'interessato[115]. Venendo alla dimensione qualitativa, il GDPR impone che, per assicurare la tutela dell'interessato e la conformità alla legge del trattamento, le loro informazioni vengano per quanto più possibile private del loro potere identificativo[116].

Secondo l'art. 5, cioè, un'informazione personale non può essere utilizzata per uno scopo per il conseguimento del quale non sia strettamente necessaria, ma anche qualora un'informazione risulti indispensabile, questa deve essere trattata in modo da limitarne al massimo l'impatto sulla privacy dell'interessato[117]. Per ottenere questo secondo obiettivo, il titolare dovrà allora utilizzare, ogni qual volta sia possibile, le tecniche che consentano di diminuire il potere identificativo dei dati, tra le quali la minimizzazione e la *privacy by default*.

È proprio qui che risiede la portata innovativa del Regolamento quanto alla minimizzazione: l'aver esplicitato, attraverso l'art. 25, la *ratio* insita nell'art. 5: ovvero che, in un contesto dinamico caratterizzato dai *big data*, dai loro sempre più vari utilizzi e dall'incessante sviluppo tecnologico, l'attenzione alla dimensione qualitativa delle informazioni e dei loro trattamenti diventa elemento rilevante per determinare la liceità della condotta dei titolari[118].

2.2.4 *Accountability* e necessità di supporto: il *Data Protection Officer*

Finora abbiamo analizzato in particolare i principi che definiscono l'atteggiamento necessario affinché il titolare operi in conformità al Regolamento, ma quali sono, in pratica, gli strumenti principali che consentano

---

campi del modulo non sono tutti necessari per l'acquisto e la spedizione dei libri. In questo caso specifico, se l'interessato paga il prodotto in anticipo, la sua data di nascita e il suo numero di telefono non sono necessari per l'acquisto. Ciò significa che questi campi del modulo web non devono essere necessariamente compilati per ordinare il prodotto, a meno che il titolare possa dimostrare chiaramente che la loro compilazione è altrimenti indispensabile, e per quali motivi. Inoltre, vi sono situazioni in cui l'indirizzo non è necessario. Per esempio, quando si ordina un e-book, il cliente può scaricare il prodotto direttamente sul proprio dispositivo. Il proprietario decide quindi di creare due moduli web: uno per ordinare i libri con un campo contenente l'indirizzo del cliente e un altro per ordinare gli e-book senza il campo dell'indirizzo".

[114] Cfr. RICCIO, G. M. & AL., *GDPR e normativa privacy*, cit., p. 250.

[115] *Ibidem*.

[116] *Ibidem.*

[117] *Ibidem*.

[118] *Ibidem*.

di dimostrate che il trattamento sia in regola con le disposizioni?

Tra le misure tecniche possiamo annoverare sicuramente l'approccio *privacy by design*[119] e la *privacy by default*[120] come elementi di particolare rilievo. Possiamo poi aggiungere la pseudonimizzazione, la trasparenza riguardo alle modalità e alle finalità del trattamento e la concessione all'interessato di controllare la correttezza dei dati[121].

Tra le misure organizzative troviamo la messa in atto di procedure che orientino le attività degli incaricati al trattamento e di politiche interne che inducano al rispetto del Regolamento[122]. L'importanza di queste procedure sta nel fatto che stabiliscono i comportamenti corretti ed evitano di lasciare gli operatori nell'incertezza quando sono chiamati ad assumere decisioni rilevanti nell'ambito del trattamento[123].

Tra queste procedure ne troviamo sicuramente una (o più d'una) per la gestione dei *data breaches*[124], nella quale siano individuati *ex ante* i casi in cui notificare la violazione all'Autorità indipendente, i soggetti da informare tempestivamente e altre indicazioni nella gestione del problema[125].

In generale, la definizione *ex ante* di procedure corrette per il trattamento costituisce un elemento di grande rilievo per dimostrare la volontà del titolare di osservare le disposizioni normative in materia. Ne consegue che la *formazione* di tutti gli incaricati al trattamento[126] sia un elemento fondamentale, come anche ribadito dall'art. 29: "*Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal*

---

[119] V. *supra*, cap. 2, § 2.2.

[120] V. *supra,* cap. 2, § 2.2.3.

[121] L'elenco è chiaramente esemplificativo. Cfr. MODAFFERI F., *Il regime particolare dei trattamenti dati effettuati per l'esecuzione di un compito di interesse pubblico*, in PIZZETTI F. & AL., *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino, Giappichelli, 2021, p. 378.

[122] V. art. 24, Regolamento 2016/679/UE.

[123] Cfr. MODAFFERI F., *Il regime particolare dei trattamenti dati effettuati per l'esecuzione di un compito di interesse pubblico*, in PIZZETTI F. & AL., *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino, Giappichelli, 2021, pp. 378 s.

[124] L'espressione viene tradotta, nella versione ufficiale italiana del Regolamento, in "violazioni di dati personali".

[125] Cfr. MODAFFERI F., *Il regime particolare dei trattamenti dati effettuati per l'esecuzione di un compito di interesse pubblico*, in PIZZETTI F. & AL., *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino, Giappichelli, 2021, p. 379.

[126] Ovvero, dal momento che l'art. 4, Regolamento 2016/679/UE include nella definizione di trattamento anche la consultazione, sostanzialmente tutti coloro che vengono a contatto con i dati.

titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri"[127].

Sorge però un problema: com'è possibile portare quella che ormai assume le caratteristiche di una vera e propria cultura della tutela dei dati personali all'interno di un contesto lavorativo, sia esso un'azienda privata o un ente pubblico, nel quale sia i vertici, sia i semplici operatori, non hanno mai avuto nulla a che fare con il tema della privacy?

Una possibile risposta a questa domanda è costituita dalla "nuova"[128] figura del *Data Protection Officer* (*DPO*) che, designato da un'azienda o un ente pubblico in funzione della conoscenza approfondita della normativa e delle prassi in materia di *data protection*, ha tra i suoi compiti quello di fornire consulenza al titolare in tutte le fasi del trattamento e sensibilizzare gli incaricati anche attraverso attività di formazione[129].

[127] Cfr. MODAFFERI F., *Il regime particolare dei trattamenti dati*, cit., p. 379.

[128] V. s*upra,* cap. 1, § 1.2.4. e *infra*, cap. 3, § 3.1.

[129] Cfr. MODAFFERI F., *Il regime particolare dei trattamenti dati*, cit., pp. 379 s.

Capitolo 3: il *Data Protection Officer*

3.1 Una parziale novità.

Il *Data Protection Officer* (*DPO*)[1] è una delle nuove figure chiave introdotte dal GDPR[2], delineato come un esperto di *data protection* che agisce sia a difesa dei diritti degli interessati, sia a supporto del titolare, del quale è consulente[3].

La figura non rappresenta però un *quid novi* assoluto, dal momento che ruoli dalle caratteristiche simili erano già previsti dalle legislazioni nazionali di alcuni Paesi europei ben prima dell'approvazione del Regolamento. Inoltre, come abbiamo visto[4], già la Direttiva 95/46/CE aveva istituito il *privacy officer* come eccezione alla notificazione all'Autorità garante della messa in opera dei trattamenti[5]. Andiamo però con ordine.

3.1.1 Nelle legislazioni nazionali

In Germania, la legge federale in materia di dati personali che nel 1990[6] sostituì il *Bundesdatenschutzgesetz* (BDSG) del 1977[7] istituì la figura del *Beauftragter für den Datenschutz* (*BfD*)[8] agli artt. 36 e 37, poi riversatisi nell'art. 4 parr. f, g della terza versione del *BDSG* del 2003[9] che recepiva le nuove legislazioni comunitarie in materia[10]. L'art. 4, par. f, sanciva l'obbligo di designazione per gli enti pubblici che trattavano informazioni personali in modo automatizzato e per privati che impiegavano almeno nove dipendenti con contratto a tempo indeterminato nel trattamento attraverso l'utilizzo di sistemi automatici[11]. La nomina era inoltre obbligatoria

---

[1] La versione italiana ufficiale del Regolamento 2016/679/UE traduce in "*Responsabile della protezione dei dati (RPD)*".

[2] Cfr. RICCIO, G. M. & AL., *GDPR e normativa privacy*, cit., p. 341.

[3] Cfr. GRECO A., *La nuova figura del data protection officer (Dpo) nell'Ue*, in *Media laws. Rivista di Diritto dei Media*, fasc. 1/2021, p. 303.

[4] V. *supra*, cap. 1, § 1.2.4.

[5] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati*, cit., p. 98.

[6] L. 29 dicembre 1990, n. 73 – *Bundesdatenschutzgesetz*, in https://www.datenschutz-wiki.de/BDSG_1990.

[7] V. *supra*, cap. 1, § 1.1.4.

[8] Anche in questo caso, la traduzione, questa volta automatica, è "Responsabile della protezione dei dati".

[9] L. 14 gennaio 2003, n. 3 – *Bundesdatenschutzgesetz*, in https://www.bgbl.de/xaver/.bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl103s0066.pdf%27%5D__1651483786026.

[10] Cfr. GRECO A., *La nuova figura del data protection officer (Dpo) nell'Ue*, cit., p. 304.

[11] Art. 4, par. f, l. federale tedesca 14 gennaio 2003, n. 3. Cfr. GRECO A., *La nuova figura del data protection officer (Dpo)*, cit., p. 304.

in tutti i casi in cui venivano impiegate almeno 20 persone nel trattamento, anche non automatizzato, dei dati[12]. Secondo tale norma, il *BfD* doveva possedere conoscenze specialistiche in materia di *data protection* e mantenere il riserbo su tutto il suo operato, motivo per cui egli doveva essere subordinato direttamente al più alto grado possibile dell'organigramma interno dell'azienda o dell'ente pubblico in cui operava[13]. Inoltre, le organizzazioni che designavano un *BfD* erano obbligate a supportarlo nello svolgimento dei suoi compiti al massimo delle proprie possibilità, fornendogli ogni attrezzatura e risorsa necessaria[14]. Quanto appena enunciato riguarda il tema dell'indipendenza del responsabile della protezione dati, tema che costituisce oggi uno dei principali argomenti di dibattito intorno alla figura del *DPO*, come vedremo di qui a poco[15].

Il par. g dello stesso art. 4 era invece dedicato ai compiti del *BfD*, il quale doveva controllare che i trattamenti fossero effettuati in conformità con il *Bundesdatenschutzgesetz*, con particolare riferimento ai programmi informatici utilizzati per trattare i dati. L'altro compito del *BfD* era di aiutare tutti gli operatori coinvolti nel trattamento a familiarizzare con la medesima legge federale e tutte le altre disposizioni in materia di *data protection*[16].

Infine, il *BfD* era chiamato a rivolgersi all'autorità di controllo, istituita già dalla prima versione del *Bundesdatenschutzgesetz* del 1977[17], in caso di necessità nello svolgimento dei propri compiti[18].

Sicuramente il *BfD* tedesco è stato il modello principale a cui il legislatore europeo si è ispirato nel delineare le caratteristiche del *Data Protection Officer* poi introdotto dal GDPR[19].

Nel 1999, in "parziale"[20] ricezione della Direttiva 95/46/CE, fu introdotta in Spagna la figura del *Responsable de seguridad*, molto simile al *BfD* tedesco, avente il compito di coordinare e controllare le misure di sicurezza

---

[12] *Ibidem*.

[13] *Ibidem*.

[14] *Ibidem*.

[15] V. *infra*, cap. 3, § 3.2.4.

[16] Art. 4, par. g, l. federale tedesca 14 gennaio 2003, n. 3. Cfr. GRECO A., *La nuova figura del data protection officer (Dpo)*, cit., p. 304.

[17] V. s*upra*, cap. 1, § 1.1.4.

[18] Art. 4, par. g, l. federale tedesca 14 gennaio 2003, n. 3. Cfr. GRECO A., *La nuova figura del data protection officer (Dpo)*, cit., p. 304.

[19] Cfr. GRECO A., *La nuova figura del data protection officer (Dpo)*, cit., pp. 304 s.

[20] In questo caso, la legislazione spagnola non si limitò a recepire la direttiva in questione senza apporre alcuna modifica, ma introdusse nel proprio ordinamento una figura con alcune caratteristiche diverse rispetto al *privacy officer* proposto dalla direttiva comunitaria: v. *supra*, cap. 1, § 1.2.4.

applicabili quando un trattamento coinvolgesse dati sensibili[21]. Altro compito del *Responsable de seguridad* era analizzare le relazioni di verifica sullo stato di sicurezza dei trattamenti, eventualmente indicando al responsabile[22] quali migliorie apportare alle misure già predisposte[23].

Elemento distintivo rispetto all'ordinamento tedesco del 1990 e del 2003 è che in Spagna l'obbligatorietà della nomina del *Responsable de seguridad* era legata non alle dimensioni del titolare del trattamento, ma alle caratteristiche dei dati trattati[24], elemento che ritroviamo nel GDPR.

3.1.2 Nelle fonti comunitarie antecedenti al GDPR

Venendo alle fonti comunitarie, possiamo trovare un primo antesignano del *Data Protection Officer* nel *privacy officer* previsto dall'art. 18, Direttiva 95/46/CE che gli Stati membri potevano istituire in fase di ricezione come misura di semplificazione alternativa all'obbligo di notifica dei trattamenti automatizzati all'Autorità di controllo competente[25]. Il responsabile[26] poteva demandare al *privacy officer* i compiti di compilazione di un registro dei trattamenti e di controllo sulla conformità alla Direttiva di quest'ultimi[27].

Un passo fondamentale nello sviluppo di questa figura ibrida di consulenza e controllo avvenne con l'emanazione del regolamento comunitario 2001/45/CE rivolto a istituzioni e organismi comunitari[28], la cui intera sezione VIII era dedicata a delineare le caratteristiche della figura del *data protection officer.*

Con il regolamento 2001/45/CE la nomina di un *DPO* fu resa obbligatoria per ogni istituzione e organismi della Comunità, affidandogli funzioni ben più ampie rispetto a quelle previste per il *privacy officer* dalla Direttiva[29].

A questa prima versione di *DPO* erano affidate le funzioni di informare responsabili e interessati dei loro

---

[21] Cfr. GRECO A., *La nuova figura del data protection officer (Dpo)*, cit., pp. 305 s.

[22] Si fa qui riferimento alla figura individuata dalla Direttiva 95/46/CE.

[23] Cfr. GRECO A., *La nuova figura del data protection officer (Dpo)*, cit., p. 306.

[24] *Ivi*, p. 307.

[25] V. *supra*, cap. 1, § 1.2.4.

[26] Si fa qui riferimento alla figura individuata dalla Direttiva 95/46/CE.

[27] *Ibidem*.

[28] Formalmente *Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali* dati, in https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32001R0045.

[29] Cfr. GRECO A., *La nuova figura del data protection officer (Dpo)*, cit., pp. 307 s.

diritti[30], cooperare con il Garante europeo della protezione dei dati[31] quando richiesto[32], garantire "*in maniera indipendente*"[33] l'applicazione delle disposizioni del regolamento stesso all'interno dell'istituzione di cui faceva parte[34], tenere un registro dei trattamenti effettuati, riguardo ai quali doveva essere informato dal responsabile *preventivamente* alla messa in atto[35], notificare al Garante europeo per la protezione dei dati la messa in atto di trattamenti che presentavano rischi specifici[36].

I successivi paragrafi dell'art. 24 statuivano che il *DPO* dovesse essere scelto "*in funzione delle sue qualità personali e professionali e, in particolare, delle sue conoscenze specifiche in materia di protezione dei dati*"[37], con un contratto di durata da due a cinque anni, rinnovabile per un totale massimo di dieci[38].

Soprattutto, la sua nomina non poteva dar luogo a conflitti d'interesse rispetto ad eventuali altri incarichi da lui ricoperti[39]; ciò, in aggiunta al divieto per le istituzioni di impartirgli istruzioni[40] e all'obbligo per le medesime di garantirgli tutte le risorse necessarie allo svolgimento dei suoi compiti[41], ne garantiva l'indipendenza da qualsiasi tipo di pressione interna[42].

Quanto detto lascia trasparire la chiara preferenza del legislatore verso un soggetto che ricoprisse esclusivamente il ruolo di *DPO* poiché, designando un dipendente già impegnato in altre mansioni si sarebbe difficilmente evitato il problema del conflitto di interessi[43].

Inoltre, considerando anche le indicazioni dell'unico allegato[44] al regolamento 2001/45/CE, il legislatore

---

[30] V. art. 24, par. 1a, regolamento 2001/45/CE.

[31] Istituita dall'art. 2, par. 2 del medesimo regolamento.

[32] V. art. 24, par. 1b, regolamento 2001/45/CE.

[33] Art. 24, par. 1c, regolamento 2001/45/CE.

[34] V. art. 24, par. 1c, regolamento 2001/45/CE.

[35] V. art. 24, par. 1d, e artt. 25, 26, Regolamento 2001/45/CE.

[36] V. art. 24, par. 1e, e art. 27, Regolamento 2001/45/CE.

[37] Art. 24, par. 2, regolamento 2001/45/CE.

[38] V. art. 24, par. 4, regolamento 2001/45/CE.

[39] V. art. 24, par. 3, regolamento 2001/45/CE.

[40] V. art. 24, par. 7, regolamento 2001/45/CE.

[41] V. art. 24, par 6, regolamento 2001/45/CE.

[42] Cfr. GRECO A., *La nuova figura del data protection officer (Dpo)*, cit., p. 308.

[43] *Ibidem.*

[44] Non lo riportiamo per brevità, ma è disponibile in calce a questa pagina: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32001R0045.

sembra propendere per la soluzione di un *DPO* esterno all'istituzione, così da evitare al meglio il conflitto di interessi e da garantirne l'indipendenza, più facilmente perseguibile con questa soluzione piuttosto che da un dipendente interno, inferiore gerarchicamente al responsabile del trattamento che era chiamato a controllare[45]. Nonostante l'atto normativo appena analizzato avesse introdotto delle novità estremamente rilevanti per la figura in questione, il suo limitato ambito di applicazione[46] ha posto un freno alla diffusione del *DPO*, pur costituendo un buon banco di prova in vista del GDPR[47].

3.2 Il *Data Protection Officer* nel Regolamento 2016/679/UE

Il *DPO* del Regolamento 2016/679/UE affonda le sue radici nella precedente versione del regolamento 2001/45/CE, ma viene arricchito di una serie di caratteristiche volte soprattutto a migliorarne le competenze di valutazione preventiva del rischio[48]. Proprio a questo proposito si ricorda che, come illustrato nel capitolo precedente, la gestione del rischio è stata totalmente rivoluzionata con l'introduzione del principio di *accountability* da parte del nuovo Regolamento. Proprio per questo, vista la radicale modifica del contesto in cui opera, anche alcune caratteristiche del DPO hanno assunto una valenza diversa.

3.2.1 Designazione

Secondo quanto stabilito dal Regolamento 2016/679/UE, la nomina del *DPO* è obbligatoria in tre casi: quando "*il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali*"[49]; quando "*le attività principali*[50] *del titolare*

---

[45] Cfr. GRECO A., *La nuova figura del data protection officer (Dpo)*, cit., p. 308.

[46] Ricordiamo che il Regolamento 2001/45/CE si applica solo agli organismi e istituzioni comunitarie.

[47] Cfr. GRECO A., *La nuova figura del data protection officer (Dpo)*, cit., p. 309.

[48] Cfr. *Ibidem* e AVITABILE A., *Il data protection officer*, in FINOCCHIARO G., *Il nuovo Regolamento europeo sula privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2020, p. 331.

[49] Art. 37, par. 1a, Regolamento 2016/679/UE.

[50] Il WP29 ha suggerito che la nozione di attività principali "*non va interpretata nel senso di escludere quei casi in cui il trattamenti di dati costituisce una componente inscindibile dalle attività svolte dal titolare del trattamento*", cfr. Article 29 Working Party, *Linee-guida sui responsabili della protezione dei dati (RPD)*, WP243 rev. 1, Bruxelles, 13/12/2016, versione emendata e adottata 05/04/ 2017, p. 9. Nello stesso documento viene proposto l'esempio di un ospedale, la cui attività principale è l'assistenza sanitaria, la quale non sarebbe però possibile senza un ampio trattamenti dei dati personali dei pazienti (tra l'altro includendo anche dei dati sensibili): quindi nel caso presentato la nomina di un *DPO* è obbligatoria.

del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala[51]"[52]; infine, quando le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di dati sensibili[53] o riguardanti condanne penali e reati[54].

Nonostante il Regolamento europeo sia un atto di natura *self-executing*, il legislatore ha comunque lasciato spazio agli Stati per adottare norme aggiuntive, purché conformi alle proprie. L'Italia ha arricchito il proprio quadro normativo mediante il d.lgs. di armonizzazione n. 101 del 2018[55] che ha modificato il precedente "Codice privacy" del 2003[56], adeguandolo alla nuova normativa europea[57].

La figura del *Data Protection Officer* era quasi del tutto sconosciuta[58] alla normativa italiana, la quale, ricordiamo, non si era avvalsa della possibilità di derogare all'obbligo di notifica dei trattamenti all'Autorità di controllo mediante il *privacy officer*, prevista dalla Direttiva 45/96/CE[59].

Nella ricezione del Regolamento, il d.lgs. 101/2018 estende l'obbligo di nomina del *DPO* anche per i

---

[51] Anche l'interpretazione di larga scala ha destato alcune perplessità nei commentatori. Nelle prime proposte del Regolamento, si faceva riferimento ad un numero di dipendenti minimo (sulla falsa riga dell'ordinamento tedesco, v. *supra*, cap. 3, § 3.1.1) stabilito a 250, raggiunto il quale sarebbe scattato l'obbligo di nomina del *DPO*. Il WP29 rilevò però che rispetto al numero di dipendenti dell'azienda, sarebbe stato più opportuno utilizzare la natura e la mole di dati, o il numero di interessati coinvolti, come criterio per stabilire l'obbligatorietà della nomina, cfr. GRECO A., *La nuova figura del data protection officer (Dpo)*, cit., p. 310.
Quanto al significato specifico dell'espressione, il c91 definisce come trattamenti su larga scala quelli "c*he mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato*". Anche in questo caso manca un'indicazione precisa in termini numerici.

[52] Art. 37, par. 1b, Regolamento 2016/679/UE.

[53] "C*ategorie particolari di dati personali di cui all'articolo 9*", art. 37, par. 1c, Regolamento 2016/679/UE.

[54] V. art. 37, par. 1c, Regolamento 2016/679/UE.

[55] D.lgs. 10 agosto 2018, n. 101 – *Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2019/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*.

[56] D.lgs. 30 giugno 2003, n. 196 – *Codice in materia di protezione dei dati personali*.

[57] Cfr. GRECO A., *La nuova figura del data protection officer (Dpo)*, cit., p. 314.

[58] Una parte della dottrina ha visto un antenato della figura in questione nel Responsabile per la prevenzione della corruzione e della trasparenza, disciplinato dal d.lgs. del 8 giugno 2001, n. 231 - *Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*. Inoltre, nonostante l'assenza di una normativa specifica, l'Autorità Garante ha anticipato il futuro contenuto del GDPR, individuando nel nuovo *Data Protection Officer* uno degli strumenti più concreti per assicurare il rispetto della normativa in materia di privacy, oltre che per superare la logica della notificazione. Cfr. SORO, A., BARBAROSSA, M. & CASSANO, G., *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, Milano, Giuffrè Francis Lefebvre, 2018, p. 176.

[59] Cfr. GRECO A., *La nuova figura del data protection officer (Dpo)*, cit., p. 314. V. *supra*, cap. 1, § 1.2.4.

"*trattamenti di dati personali effettuati dalle autorità giudiziarie nell'esercizio delle loro funzioni*"[60], contravvenendo all'eccezione prevista all'art. 37, par. 1a del Regolamento 2016/679/UE, che abbiamo riportato poche righe sopra[61].

In realtà, l'eccezione prevista dal Regolamento non determina la creazione di alcuna lacuna, dal momento che lo stesso testo esclude l'applicazione di tutte le regole in sé contenute ai trattamenti effettuati per ragioni di giustizia dalle autorità giudiziarie[62], in ragione dell'esistenza di uno specifico atto dell'Unione riguardante il trattamento dei dati personali effettuati da questo tipo di autorità: la Direttiva 2016/680/UE, la quale contiene una sezione dedicata al *DPO* in contesti di autorità giurisdizionali[63].

Tale sezione, composta dagli artt. 32 - 34, prescrive l'obbligo per le autorità giudiziarie di "*nominare un DPO incaricato dello svolgimento di compiti consultivi, di sorveglianza e di cooperazione, analoghi a quelli previsti dal Regolamento*"[64].

Data l'esistenza di questo più specifico atto, peraltro già recepito in Italia mediante il d.lgs. 18 maggio 2018, n. 51, una parte dei commentatori è rimasta perplessa[65] di fronte all'inserimento nel Codice privacy dell'art. 2-*sexiesdecies*, il quale è per di più sprovvisto di un riferimento al d.lgs. 51/2018, definendolo una "*'sbavatura' del sistema*"[66]. ''''

Tornando alla figura del *Data Protection Officer* del GDPR, quand'anche la sua nomina non sia obbligatoria, il WP29 ne consiglia la designazione[67] come parte delle iniziative volontarie che costituiscono il secondo livello dell'*accountability*[68]. Ad ogni modo, tutti i titolari (o i responsabili) sono tenuti a documentare ed essere in grado di dimostrare le valutazioni effettuate per decidere se si applichi o meno l'obbligo di nomina di un

---

[60] Art. 2-*sexiesdecies*, d.lgs. 30 giugno 2003, n. 196, c.d. "Codice privacy", aggiornato dal d.lgs. 10 agosto 2018, n. 101.

[61] Cfr. CARAVÀ E. & SCIAUDONE R., *Il codice della privacy: commento al D.Lgs. 30 giugno 2003, n. 196 e al D.Lgs 10 agosto 2018, n. 101 alla luce del Regolamento (UE) 2016/679 (GDPR)*, Pisa, Pacini Giuridica, 2019, pp. 186 s.

[62] V. Considerando 19, Regolamento 2016/679/UE. *Ibidem.*

[63] Cfr. CARAVÀ E. & SCIAUDONE R., *Il codice della privacy*, cit., p. 187.

[64] *Ibidem.*

[65] *Ivi*, pp. 187 s.

[66] *Ivi*, p. 188.

[67] Article 29 Working Party, *Linee-guida sui responsabili della protezione dei dati (RPD)*, WP243 rev. 1, Bruxelles, 13/12/2016, versione emendata e adottata 05/04/ 2017, p. 3.

[68] V. *supra*, cap. 2, § 2.1.3. Tale possibilità è anche esposta all'art. 37, par. 4, Regolamento 2016/679/UE.

DPO all'interno della propria organizzazione[69].

Come esplicitato nei parr. 2 e 3 dell'art. 37, più enti pubblici, o aziende private appartenenti allo stesso gruppo imprenditoriale, possono nominare un unico *DPO*, a patto che la struttura organizzativa, la dimensione e la geolocalizzazione dei diversi soggetti designanti consentano uno svolgimento scrupoloso delle attività previste[70].

Proseguendo nella lettura dell'art. 37, troviamo un paragrafo molto simile al par. 2 dell'art. 24 del regolamento 2001/45/CE, riguardante le qualità professionali e le conoscenze in funzione delle quali deve essere scelto il *DPO*[71]; non vengono invece citate le qualità personali[72]. Inoltre, i recapiti del *DPO* designato devono essere pubblicati e inclusi nell'informativa per il consenso[73].

Il par. 6 dell'art. 37 introduce un tema che è stato oggetto di numerose discussioni: viene infatti espressa la possibilità, per un titolare, di nominare *DPO* un dipendente interno all'organizzazione (*DPO* interno) o di scegliere un soggetto esterno tramite un contratto di sevizi (*DPO* esterno).

Naturalmente la scelta è da effettuarsi in base al contesto in esame, ma si possono delineare alcuni pro e contro generali a ciascuna delle due soluzioni[74]. Sicuramente un *DPO* interno ha il vantaggio di conoscere più approfonditamente i dettagli dell'azienda/ente in cui opera; inoltre, sarà tendenzialmente più facile da contattare in caso di necessità[75].

Di contro, un DPO esterno avrà più facilmente garantite l'autonomia e l'assenza di istruzioni, sarà facilitato nel rivolgersi alle figure apicali della struttura e gestirà in proprio i costi del proprio aggiornamento professionale, risparmiandoli all'azienda[76]. Soprattutto però, un DPO esterno non sarà mai coinvolto in scelte

---

[69] Cfr. RICCIO, G. M. & AL., *GDPR e normativa privacy*, cit., p. 343. Per un caso concreto v. *infra.*

[70] Cfr. BONGIOVANNI S., MOTTINO C. & PEREGO M., *Il formulario del DPO: norme, giurisprudenza, strumenti operativi e modelli di atti*, Torino, Giappichelli, 2021, pp. 12 s.

[71] V. *infra*, cap. 3, § 3.2.2.

[72] Le "*qualità personali*" venivano citate nell'art. 24, par. 2 del Regolamento 2001/45/CE come un elemento da valutare, insieme a quelle professionali, nella scelta di un *DPO.*

[73] V. art. 37, par. 7, Regolamento 2016/679/UE.

[74] Cfr. BONGIOVANNI S., MOTTINO C. & PEREGO M., *Il formulario del DPO: norme, giurisprudenza, strumenti operativi e modelli di atti*, Torino, Giappichelli, 2021, p. 10.

[75] *Ibidem*.

[76] *Ibidem.*

di carattere operativo o strategico che possano configurare una condizione di conflitto di interessi[77], tema che analizzeremo in seguito[78].

Essendo la nomina di una figura a protezione dei dati personali divenuta obbligatoria, sono state introdotte anche delle sanzioni per chi non la completa[79]. Ad esempio, nell'agosto 2019, l'Autorità austriaca ha sanzionato una clinica privata a causa di una serie di inadempimenti, tra i quali la mancata nomina del *DPO*, con un'ammenda di € 51.000[80]. Nello stesso anno, l'Autorità spagnola ha sanzionato la società Glovoapp23 SL a seguito di una serie di reclami degli utenti per l'assenza nell'informativa dei recapiti del *DPO*. In risposta, la società ha inizialmente dichiarato di non essere soggetta all'obbligo di nomina, pur avendo delegato alcuni compiti previsti dall'art. 39[81] al personale interno. Successivamente, la società ha comunque nominato un *DPO*, ma il ritardo è stato comunque motivo di una sanzione di € 25.000[82].

3.2.2 Requisiti necessari per la nomina

Visto quanto precede, diventa allora rilevante individuare l'insieme di conoscenze e competenze che un soggetto debba possedere per essere nominato *Data Protection Officer*.

Come espresso all'art. 37, par. 5, il *DPO* viene designato in funzione delle sue qualità professionali, con particolare riferimento alla conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati[83]. Questo par. ricalca il par. 2, art. 24 del Regolamento 45/2001/CE[84] attorno al quale si è da tempo formata una prassi che individua un'esperienza rilevante di almeno 3 anni nel settore della *data protection* come una

---

[77] *Ivi*, p. 11.

[78] V. *infra*, cap. 3, § 3.2.4.

[79] L'art. con cui il GDPR definisce le sanzioni è l'83, nel par. 4 del quale troviamo: "L*a violazione delle disposizioni seguenti [tra le quali sono presenti gli artt. 37 - 39] 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*". Le sanzioni devono essere inflitte tenendo conto di una serie di elementi (tra cui le caratteristiche dell'azienda o dell'ente) descritti nei parr. precedenti dell'art. 83, che non riportiamo per brevità.

[80] V. BONGIOVANNI S., MOTTINO C. & PEREGO M., *Il formulario del DPO*, cit., p. 11.

[81] Questo articolo contiene i compiti che un *DPO* deve svolgere, v. *infra*, cap. 3, § 3.2.3.

[82] V. BONGIOVANNI S., MOTTINO C. & PEREGO M., *Il formulario del DPO*, cit., p. 11. V. anche *Agencia Española de Protecctión de Datos*, procedimento PS/00417/20189, in https://www.aepd.es/es/documento/ps-00417-2019.pdf, trad. automatica in https://gdprhub.eu/index.php?title=AEPD_-_PS/00417/2019#Comment.

[83] Cfr. SORO, A., BARBAROSSA, M. & CASSANO, G., *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, Milano, Giuffrè Francis Lefebvre, 2018, p. 189.

[84] V. *supra*, cap. 3, § 3.1.2.

delle qualità professionali essenziali per la figura in questione[85].

Ancora meglio, come indicato dal WP29 nelle linee guida sul *DPO*[86], se l'esperienza del candidato è maturata all'interno del settore specifico a cui appartiene la struttura organizzativa del titolare, utilizzando i medesimi sistemi informativi con specifiche esigenze di sicurezza e protezione dei dati. Nello stesso documento, viene richiesto al titolare o al responsabile di valutare anche le qualità personali[87] del candidato.

È chiaro che qualora il *DPO* nominato non dovesse disporre dei requisiti imposti dalla normativa, non si potrebbe ritenere assolto l'obbligo di nomina, comportando l'applicazione di sanzioni in caso di verifica da parte dell'Autorità di controllo[88].

In questo senso è bene porre attenzione su eventuali certificazioni e attestazioni che un candidato potrebbe avere ottenuto attraverso attività o corsi specifici. In generale, si consideri che il GDPR si è espresso favorevolmente[89] all'adozione di codici di condotta di categoria e a certificazioni quali *step* di un percorso di *accountability*[90]. Di conseguenza anche la designazione di un *DPO* che possiede competenze professionali certificate da un soggetto terzo può essere percepita come un ulteriore elemento di responsabilizzazione[91].

Su questo tema è però intervenuta l'Autorità Garante italiana, attraverso la newsletter n. 432 del 15 settembre 2017, nella quale si legge che, in conformità con le indicazioni del legislatore europeo, l'attestazione delle qualità professionali richieste non richieda il possesso di particolari certificazioni, anche se queste possono costituire validi elementi per valutare il possesso di un livello adeguato di conoscenza[92].

A conferma di ciò, il Tribunale Amministrativo Regionale per il Friuli-Venezia Giulia si è pronunciato, primo

---

[85] Cfr. SORO, A., BARBAROSSA, M. & CASSANO, G., *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, Milano, Giuffrè Francis Lefebvre, 2018, p. 189.

[86] Cfr. Article 29 Working Party, *Linee-guida sui responsabili della protezione dei dati (RPD)*, WP243 rev. 1, Bruxelles, 13/12/2016, versione emendata e adottata 05/04/ 2017, p. 15.

[87] Le qualità personali comparivano, come elemento di valutazione in questi termini, già all'art. 24, par. 2, regolamento 2001/45/CE.

[88] Cfr. CILONA A., *I requisiti per la nomina del data protection officer e la certificazione lead auditor Iso 27001*, nota a sentenza T.A.R. Trieste, (Friuli-Venezia Giulia) sez. I, 13/09/2018, n.287, in *Media laws. Rivista di Diritto dei Media*, fasc. 1/2019, p. 244.

[89] V. artt. 42, 43, Regolamento 2016/679/UE.

[90] Cfr. GRECO A., *La nuova figura del data protection officer (Dpo)*, cit., p. 315.

[91] *Ibidem.*

[92] Cfr. SORO, A. & AL., *Il processo di adeguamento al* GDPR, cit., p. 189. V. Garante per la Protezione dei Dati Personali, Newsletter n. 432 del 15 settembre 2017, in https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6826945.

in Italia, con la sentenza del 13 settembre 2018 n. 287[93], sulla questione dei requisiti necessari per la nomina del *DPO*[94].

Nel caso in questione, il T.A.R. è stato chiamato a pronunciarsi sulla legittimità del bando di concorso di un'azienda sanitaria per l'affidamento di un incarico per il ruolo di *DPO.* Tra i requisiti per la partecipazione, il bando richiedeva il possesso del diploma di laurea in Informatica o Ingegneria informatica, ovvero in Giurisprudenza o equipollenti, e la certificazione Auditor/Lead Auditor per i Sistemi di Gestione per la Sicurezza delle Informazioni secondo la norma ISO/IEC 27001[95].

Il bando, insieme al decreto a mezzo del quale ne era stata disposta la pubblicazione, è stato impugnato con ricorso da uno dei due candidati alla selezione, il quale era laureato in Giurisprudenza ma privo della certificazione Auditor/Lead Auditor ISO/IEC 27001, prima ancora della pubblicazione del risultato del concorso[96].

Il ricorrente chiedeva l'annullamento degli atti amministrativi per, tra le altre, violazione degli artt. 37 e 39 del Regolamento 2016/679/UE e contestava la pertinenza, rispetto al ruolo del *DPO*, della certificazione in questione, la quale sarebbe stata anche causa di "*un'indebita sperequazione ai danni dei soggetti titolari della laurea in Giurisprudenza*"[97]. Inoltre, il ricorrente contestava l'ammissibilità della laurea in Informatica o in

---

[93] Il testo completo della sentenza è in https://www.giustizia-amministrativa.it/portale/pages/istituzionale/ucm?id=5LLMWH2MBE2JVPC536FUMJHNYU&q e in https://www.foroplus.it/visualizza.php?pag=1&ndoc=2262271G&sha1=2976216fe7add7e4c78ec8ae4d96690d13a22842&ur=. V. anche la nota a sentenza di CILONA A., *I requisiti per la nomina del data protection officer e la certificazione lead auditor Iso 27001*, nota a sentenza T.A.R. Trieste, (Friuli-Venezia Giulia) sez. I, 13/09/2018, n.287, in *Media laws. Rivista di Diritto dei Media*, fasc. 1/2019, pp. 240 - 246.

[94] Di seguito si analizzerà una sentenza italiana nella quale, in luogo dell'espressione inglese *Data Protection Officer,* viene utilizzata la traduzione "Responsabile della protezione dei dati (RPD)". Cfr. CANCARINI S. & AL., *Data Protection Officer: guardiano od operatore della privacy? Casi pratici aziendali nei primi sei mesi di applicazione del GDPR*, in *Corporate compliance round tables 2018 (Atti del convegno)*, a cura di PICCIANO I. & BANA A., in *I quaderni del gruppo ASLA di* corporate compliance, ASLA, 2018, Cap. I, pp. 9 - 24, (https://www.aslaitalia.it/files/pubblicazioni/2019/ASLA%20epub%20CC2018.pdf,), p. 15.

[95] In seguito "Auditor/Lead Auditor ISO/IEC 27001". Si tratta di uno standard internazionale che regola l'impostazione e il mantenimento di un sistema di gestione della sicurezza informatica. La certificazione può essere conseguita al termine di un percorso di formazione e ad un esame certificati secondo gli standard ISO (International Organization for Standardization). Dal momento che alcuni dei suoi contenuti sono sovrapponibili ai principi del GDPR in tema di sicurezza del trattamento, è diffusa l'opinione che lo standard ISO/IEC 27001 possa rappresentare un esempio di standard da seguire per trattare i dati personali in conformità al GDPR. Cfr. CILONA A., *I requisiti per la nomina del data protection officer*, cit., p. 245.

[96] Cfr. T.A.R. Trieste (Friuli-Venezia Giulia), sez. I, sentenza del 13/09/2018, n. 287, con nota di Cilona A., cit., p. 241.

[97] T.A.R. Trieste (Friuli-Venezia Giulia), sez. I, sentenza del 13/09/2018, n. 287.

Ingegneria informatica come titoli alternativi alla laurea in Giurisprudenza[98].

Respinte le formulazioni difensive dell'azienda sanitaria resistente, il Collegio ha sancito, nel merito, la fondatezza del ricorso del candidato: "*la predetta certificazione non costituisce, come eccepito dal ricorrente, un titolo abilitante ai fini dell'assunzione e dello svolgimento delle funzioni di responsabile della sicurezza dei dati, nell'alveo della disciplina introdotta dal GDPR* [...] *sicché la minuziosa conoscenza e l'applicazione della disciplina di settore restano, indipendentemente dal possesso o meno della certificazione in parola, il nucleo essenziale ed irriducibile della figura professionale ricercata mediante la procedura selettiva intrapresa dall'Azienda, il cui profilo, per le considerazioni anzidette, non può che qualificarsi come eminentemente giuridico* [...] *Ne consegue che la certificazione, indicata nell'avviso, di per sé non può costituire requisito di ammissione alla selezione in esame (né tanto meno assurgere a titolo equipollente al richiesto diploma di laurea), proprio perché essa non coglie (o non coglie appieno) la specifica funzione di garanzia insita nell'incarico conferito, il cui precipuo oggetto non è costituito dalla predisposizione dei meccanismi volti ad incrementare i livelli di efficienza e di sicurezza nella gestione delle informazioni ma attiene semmai, come rilevato nel ricorso, alla tutela del diritto fondamentale dell'individuo alla protezione dei dati personali indipendentemente dalle modalità della loro propagazione e dalle forme, ancorché lecite, di utilizzo*"[99].

3.2.3 Compiti e funzioni

Il *Data Protection Officer*, come descritto nell'art. 39 del Regolamento[100], svolge un ruolo misto di consulenza al titolare (o al responsabile) e di controllo sui processi interni alla struttura in cui opera[101].

Come consulente egli assiste il titolare e gli altri incaricati nella gestione dei trattamenti, informandoli degli obblighi prescritti dal Regolamento e dalle altre disposizioni dell'Unione o degli Stati membri[102]. Da questo punto di vista al *DPO* compete la funzione di promuovere la cultura della protezione dei dati all'interno

[98] Cfr. T.A.R. Trieste (Friuli-Venezia Giulia), sez. I, sentenza del 13/09/2018, n. 287, con nota di Cilona A., cit., p. 241.

[99] T.A.R. Trieste (Friuli-Venezia Giulia), sez. I, sentenza del 13/09/2018, n. 287.

[100] L'art. 39 descrive i compiti *minimi.*

[101] Cfr. BOLOGNINI L. & AL., *Il regolamento privacy europeo: commentario*, cit., p. 163.

[102] V. art. 39, par. 1a, Regolamento 2016/679/UE.

dell'organizzazione in cui opera[103]. Ecco perché egli interviene in ogni fase del trattamento, relazionandosi tanto con i soggetti interni come il titolare (e il responsabile), quanto con quelli esterni come gli interessati e l'Autorità di controllo[104].

Nel caso in cui la nomina avvenga preventivamente alla messa in atto dei trattamenti, il *DPO* può svolgere un ruolo chiave nella definizione degli stessi, come parte integrante dell'approccio *privacy by design*, attraverso la formulazione di pareri in merito alla valutazione d'impatto (*Data Protection Impact Assessment - DPIA*)[105] messa in atto dal titolare[106]. In questo frangente, il coinvolgimento del *DPO* è triplice: infatti egli è chiamato ad esprimersi in primo luogo sull'opportunità e l'obbligatorietà di effettuare una valutazione d'impatto; in secondo luogo, il *DPO* deve esprimersi in ordine alla possibilità di effettuare la *DPIA* internamente o esternamente all'organizzazione. Infine, al *DPO* può essere richiesto di formulare un parere sui risultati ottenuti dalla valutazione d'impatto stessa[107].

Ad ogni modo, fin da questa prima fase risulta evidente la necessità per il *DPO* di accedere a tutte le informazioni riguardanti i trattamenti e i dati personali in generale, al fine di rendere la consulenza effettiva e più efficace possibile[108]. Infatti, confrontando gli obblighi a carico del titolare del trattamento con i compiti del *DPO* emerge che se il primo deve mettere in atto le misure che abbiamo visto[109] in funzione di "*natura, ambito di applicazione, contesto e finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche*"[110], il *DPO* deve eseguire i compiti a lui affidati sulla base dei medesimi fattori[111]. È quindi indispensabile che quest'ultimo disponga di tutte le valutazioni, in forma scritta, effettuate dal titolare sul trattamento dei dati, al fine di poter considerare l'incidenza dei singoli fattori

---

[103] Cfr. AVITABILE A., *Il data protection officer*, cit., p. 348.

[104] *Ibidem*.

[105] Si riporta di seguito la definizione di valutazione d'impatto: "*Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali*". Art. 35, Regolamento 2016/679/UE.

[106] V. art. 39, par. 1c, Regolamento 2016/679/UE.

[107] Cfr. AVITABILE A., *Il data protection officer*, cit., pp. 348 s.

[108] *Ibidem.*

[109] V. *supra*, cap. 2, § 2.1.2.

[110] Art. 24, Regolamento 2016/679/UE.

[111] Cfr. BONGIOVANNI S., MOTTINO C. & PEREGO M., *Il formulario del DPO*, cit., pp. 52 s.

citati[112].

Più articolati sono invece i compiti di vigilanza, che comprendono il controllo dell'osservanza del Regolamento e delle altre disposizioni relative alla *data protection*, delle politiche del titolare o del responsabile come l'attribuzione di responsabilità, la formazione e la sensibilizzazione generale sul tema della protezione dei dati[113]. In questo senso risulta evidente che per operare con maggior efficacia in situazioni di "*incident handling*"[114] e "*incident response*"[115], il *DPO* debba avere la capacità e disporre delle risorse per effettuare ispezioni, consultazioni, attività di documentazione e analisi dei registri[116].

Anche per quanto riguarda questo secondo gruppo di funzioni vale quanto detto in precedenza riguardo al rapporto tra gli obblighi del titolare e le mansioni del *DPO*. Ancora una volta queste due figure sembrano, nel sistema definito dal GDPR, essere state concepite in modo speculare: idealmente, infatti, un titolare che incarna appieno le logiche dell'*accountability* deve tenere traccia di ogni sua valutazione e decisione riguardo alla messa in atto (o non messa in atto) di un trattamento e, più in generale riguardo a qualunque decisione concernente i dati personali[117]. Si noti che il fatto che questi documenti vengano effettivamente prodotti concorre, agli occhi del legislatore, a rendere il titolare *compliant* alla normativa tanto quanto l'effettivo rispetto di quanto statuito dagli articoli del Regolamento[118].

Questi stessi documenti costituiscono il materiale fondamentale per il lavoro del *DPO*[119], che, indipendentemente dal fatto che egli svolga la funzione di "consigliere" o di "controllore", pare a chi scrive, ne sia il vero destinatario. Facendo infatti riferimento alla relazione annuale dell'attività del Garante privacy italiano[120], troviamo che i riscontri a reclami e segnalazioni sono circa 9000, i quali hanno portato a 148

---

[112] *Ibidem*.

[113] V. art. 39, par. 1b, Regolamento 2016/679/UE.

[114] AVITABILE A., *Il data protection officer*, cit., p. 361.

[115] *Ibidem*.

[116] Cfr. *ibidem.*

[117] V. "*rendicontazione*", *supra*, cap. 2, § 2.1.

[118] *Ibidem*.

[119] Cfr. BONGIOVANNI S., MOTTINO C. & PEREGO M., *Il formulario del DPO*, cit., pp. 52 s.

[120] V. Garante per la Protezione dei dati personali, *Relazione Annuale 2020*, in https://www.garanteprivacy.it/documents/10160/0/Relazione+annuale+2020.pdf/286a6332-896a-d4b1-a2da-e32d7d4838c9?version=2.0.

decisioni, mentre sono invece 21 le ispezioni[121]. Sebbene questi numeri testimonino l'importante lavoro dell'Autorità di controllo italiana, è chiaro che questa non può realisticamente mantenere un monitoraggio continuo delle attività di tutte le grandi organizzazioni che operano con i dati personali[122]. Ecco che in questo spazio di controllo si collocano i *DPO*, i quali sono invece pensati per agire in modo continuo e a livello di singola realtà, potendo quindi più puntualmente sfruttare le rendicontazioni prodotte dai titolari[123].

Ciò non toglie che nello svolgere i suddetti compiti, il *DPO* deve cooperare con l'Autorità di controllo di riferimento e fungere per essa da primo punto di contatto all'interno dell'azienda, soprattutto riguardo a questioni connesse al trattamento, ricorrendo, se necessario, a delle consultazioni[124].

In questo senso, assumono importanza le caratteristiche di professionalità e reperibilità che costituiscono due requisiti necessari alla nomina, in quanto il *DPO* dovrà interfacciarsi con l'Autorità di controllo, ad esempio, durante la gestione dei *data breaches*. Non solo, i rapporti tra il *DPO* e l'Autorità di controllo possono concretizzarsi in verifiche preliminari (art. 17, Codice privacy), anche in conseguenza dei risultati della DPIA, in richieste di autorizzazioni e anche nell'ambito di accertamenti e controlli di iniziativa dell'Autorità stessa[125].

Ad ogni modo, proprio in virtù del carattere non esaustivo dell'elenco di compiti individuati dall'art. 39 del Regolamento, il titolare o il responsabile possono assegnare al *DPO* ulteriori compiti, come delegargli il mantenimento di un registro di operazioni di trattamento che, in prima istanza, rientrerebbe tra i compiti dei primi due[126]. Nella prassi reale potrebbe essere, infatti, il *DPO* a realizzare l'inventario dei trattamenti ed a tenerne un registro basato sulle informazioni fornitegli dai vari dipartimenti aziendali[127].

---

[121] Per completezza si vedano anche i report relativi agli anni precedenti in quanto, con l'avvento della pandemia da Covid-19, la frequenza di alcune tipologie di interventi è stata logicamente ridotta. L'elenco completo dei report annuali del Garante è disponibile in https://www.garanteprivacy.it/documents/10160/0/Relazione+annuale+2020.pdf/286a6332-896a-d4b1-a2da-e32d7d4838c9?version=2.0.

[122] Ci si riferisce a tutti quei soggetti identificati all'art. 37, Regolamento 2016/679/UE.

[123] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali. 2, Il regolamento europeo 2016/679*, Torino, Giappichelli, 2016, pp 108 s.

[124] V. art. 39, parr. 1d, 1e, Regolamento 2016/679/UE.

[125] Cfr. NAPOLI S., *La figura del Data Protection Officer nel nuovo Regolamente Europeo,* in *AIEA*, Maggio 2017, in http://www.aiea.it/sites/default/files/pubblicazioni/download/la_figura_del_data_protection_officer_nel_nuovo_regolamento_europeo_0.pdf, pp. 15 s.

[126] Cfr. AVITABILE A., *Il data protection officer*, cit., pp. 364 s.

[127] *Ibidem*.

Alcuni commentatori hanno definito "*amplissimi*"[128] i compiti del *DPO*: egli dovrebbe innanzitutto essere un giurista[129], esperto non solo del Regolamento, ma anche delle leggi nazionali che lo integrano; deve poi essere specializzato nei trattamenti di dati personali, per la cui completa analisi sono necessarie anche delle conoscenze approfondite di informatica. Quanto al contesto in cui opera, il *DPO* deve considerare tutti i flussi di dati all'interno dell'organizzazione del titolare e comprenderne le criticità, deve svolgere verifiche e ricopre un ruolo di supporto e gestione di crisi in caso di *data breach*[130], essere un punto di riferimento per gli interessati e per l'Autorità di controllo[131]. A ciò si aggiunge che, nell'ipotesi di un *DPO* interno, tutte queste mansioni potrebbero sommarsi con altre.

In un certo senso, sembra che la figura del *DPO* non sia stata codificata con sufficiente chiarezza da parte del legislatore, che ha lasciato ai commentatori di cui sopra la sensazione di "*un'accumulazione caotica di esigenze assai diverse tra loro, talvolta anche in potenziale conflitto*"[132]. I fautori di questo orientamento hanno dato poco credito all'ipotesi di concentrare tutte le attività previste in un'unica persona fisica, ma ritengono più realistica l'idea di concepire il *DPO* come una funzione a cui si dedicano, in team[133], più soggetti a tempo pieno[134]. Sarà anche auspicabile allora il ricorso a soggetti esterni (più facilmente personalità giuridiche) mediante il "*contratto di servizi*" previsto all'art. 37, par. 6[135].

3.2.4 Posizione, indipendenza e conflitto di interessi

Come accaduto per il regolamento 2001/45/CE, anche nel Regolamento 2016/679/UE vengono date ampie indicazioni riguardo alla posizione del *Data Protection Officer* nell'organizzazione in cui opera e alla sua indipendenza. A questi temi è dedicato l'art. 38, il quale si apre prescrivendo al titolare e al responsabile di

---

[128] BOLOGNINI L., PELINO E. & BISTOLFI C., *Il regolamento privacy europeo: commentario*, cit., p. 166.

[129] Sebbene alcune organizzazioni, una delle quali è stata per questo coinvolta in un procedimento (v. *infra*), abbiano individuato alcuni profili informatici, come alternativa ai giuristi, nell'ambito della designazione di un *DPO*, tutti gli autori citati in questo lavoro propendono per la nomina di profili primariamente giuridici per tale posizione.

[130] L'espressione si può qui tradurre in "fuga di dati".

[131] Cfr. BOLOGNINI L. & AL., *Il regolamento privacy europeo: commentario*, cit., p. 166.

[132] BOLOGNINI L. & AL., *Il regolamento privacy europeo: commentario*, cit., p. 167.

[133] Tale opzione è consentita dal legislatore, mentre è invece vietato che un titolare nomini più di un *DPO.* V. RICCIO, G. M. & AL., *GDPR e normativa privacy*, cit., p. 346.

[134] Cfr. BOLOGNINI L. & AL., *Il regolamento privacy europeo: commentario*, cit., p. 167. Questa soluzione è consigliata anche in RICCIO, G. M., SCORZA G. & BELISARO E., *GDPR e normativa privacy*, cit., p. 346.

[135] *Ibidem*.

coinvolgere tempestivamente il *DPO* in tutte le questioni riguardanti i dati personali[136].

La conseguenza più diretta è che egli debba partecipare alle riunioni di management di medio e alto livello con scadenze regolari, in particolare quando vengono prese decisioni riguardanti la *data protection*, riguardo alle quali la sua opinione deve essere tenuta in grande considerazione dal titolare (o dal responsabile)[137]. Si precisa che il titolare non è obbligato ad accettare l'opinione del *DPO*, ma, in linea con il principio di *accountability*, deve tenere traccia scritta delle ragioni che hanno portato al dissenso[138].

Il titolare e il responsabile devono garantire al *DPO* tutto il supporto necessario nello svolgimento dei suoi compiti; a quest'ultimo devono essere garantite tutte le risorse necessarie[139] per completare le proprie funzioni e per "*mantenere la propria conoscenza specialistica*"[140]: ovvero, specialmente nel caso in cui venga incaricato del ruolo un soggetto interno, l'azienda/ente deve farsi carico dei costi inerenti alla formazione continua del *DPO*[141].

Proseguendo nella lettura dell'articolo, il par. 3 introduce il concetto di *indipendenza* del *Data Protection Officer*, il quale non deve ricevere "*alcuna istruzione per quanto riguarda l'esecuzione* [dei suoi, nda] [...] *compiti*"[142]. Allo stesso modo, egli non può ricevere istruzioni su come condurre gli accertamenti su un reclamo oppure sull'opportunità di consultare l'Autorità di controllo[143].

Una delle prime soluzioni previste dal Regolamento al fine di evitare eventuali conflittualità è che il *DPO* sia subordinato direttamente al vertice gerarchico dell'organigramma[144]. È però bene ricordare che il titolare mantiene la piena responsabilità della conformità dei trattamenti alla normativa (art. 5, par. 2, Reg.)[145]: il *DPO*

---

[136] V. art. 38, par. 1, Regolamento 2016/679/UE.

[137] Cfr. RICCIO, G. M. & AL., *GDPR e normativa privacy*, cit., pp. 347 s.

[138] *Ibidem*.

[139] Le risorse sono da intendersi di ogni tipo, comprese quelle economiche, umane e specialmente quelle di tempo. In particolare, nel caso di un DPO interno sarebbe opportuno stabilire aprioristicamente la percentuale dell'orario di lavoro da destinare alla suddetta funzione. Cfr. AVITABILE A., *Il data protection officer*, in FINOCCHIARO G., *Il nuovo Regolamento europeo sula privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2020, p. 358

[140] Art. 38, par. 2, Regolamento 2016/679/UE.

[141] Cfr. BONGIOVANNI S., MOTTINO C. & PEREGO M., *Il formulario del DPO*, cit., p. 10.

[142] Art. 38, par. 3, Regolamento 2016/679/UE.

[143] Cfr. AVITABILE A., *Il data protection officer*, cit., p. 354.

[144] *Ibidem*.

[145] *Ibidem*.

non assume cioè alcuna responsabilità diretta per sanzioni da parte dell'Autorità o eventuali risarcimenti nei confronti degli interessati nel caso in cui l'azienda/ente nella quale opera fallisca nella *compliance* al Regolamento[146]. Ad ogni modo, qualora gli adempimenti alla normativa siano da imputarsi alla mancata perizia del *DPO* nello svolgimento dei suoi compiti, il titolare potrà rivalersi su di lui chiedendo un risarcimento ed eventualmente procedere al licenziamento per giusta causa[147].

Al par. 4 e dell'art. 38, si legge che il *Data Protection Officer* debba porsi come primo interlocutore per gli interessati riguardo a tutte le questioni concernenti le informazioni personali e i trattamenti, supportandoli nell'esercizio dei loro diritti[148]. Il paragrafo seguente prescrive al designato di mantenere il riserbo riguardo allo svolgimento dei propri compiti[149].

Di particolare interesse è il par. 6, che riguarda il tema del conflitto di interessi: al *Data Protection Officer* è infatti concesso di svolgere anche altri compiti rispetto a quelli espressi all'art. 37[150], a patto che "*tali compiti* [aggiuntivi, nda] *non diano adito a un conflitto di interessi*"[151]; l'assicurarsi che ciò non accada è ancora in capo al titolare (o al responsabile)[152].

L'assenza di conflitto di interessi è un requisito indispensabile affinché il *DPO* operi in modo indipendente[153]. Ciò significa che il DPO non può rivestire, all'interno della stessa organizzazione, un ruolo che contribuisca a determinare le modalità e le finalità del trattamento[154]. Il WP29 ha indicato alcuni ruoli non compatibili con la figura in questione: "*amministratore delegato, responsabile operativo, responsabile finanziario, responsabile sanitario, direzione marketing, direzione risorse umane, responsabile IT*"[155].

Allo scopo di evitare situazioni di conflitto di interessi possono concorrere anche l'individuazione preventiva, da parte del titolare o del responsabile, di quelle posizioni incompatibili con la funzione di *DPO*, la redazione

---

[146] Cfr. Article 29 Working Party, *Linee-guida sui responsabili della protezione dei dati (RPD)*, cit., p. 16.

[147] Cfr. AVITABILE A., *Il data protection officer*, cit., p. 355.

[148] V. art. 38, par. 4, Regolamento 2016/679/UE.

[149] V. art. 38, par. 5, Regolamento 2016/679/UE.

[150] V. *supra*, cap. 3, § 3.2.3.

[151] V. art. 38, par. 6, Regolamento 2016/679/UE.

[152] V. *ibidem.*

[153] Cfr. AVITABILE A., *Il data protection officer*, cit, p. 355.

[154] Cfr. Article 29 Working Party, *Linee-guida sui responsabili della protezione dei dati (RPD)*, cit., p. 17.

[155] *Ibidem.*

di un regolamento apposito in questo senso, il rilascio di una dichiarazione scritta attestante l'assenza di conflitto di interessi e l'utilizzo nei contratti di formulazioni precise e dettagliate, così da prevenire ogni problematica[156].

Se quelle appena elencate sono soluzioni pratiche, bisogna ricordare che l'indipendenza è prima di tutto un atteggiamento mentale, il quale definisce i soggetti che danno ascolto a tutti, ma senza porsi in subordinazione[157]. Potrà infatti accadere che il *DPO* si accorga che un'attività effettuata, o che si intende mettere in atto, non è conforme alle normative vigenti; nel caso sarà suo preciso dovere riportarlo ai vertici di riferimento, anche se, come nella maggior parte dei casi, ciò si contrapporrà agli interessi di chi lo ha designato[158].

Tutto ciò presuppone che il *DPO* disponga senz'altro di una solida preparazione, ma anche di "*un forte senso di responsabilità e un'elevata considerazione del proprio ruolo, specificamente finalizzato ad aumentare* [...] *le garanzie per gli interessati*"[159].

Per queste ragioni, il *Data Protection Officer* è un elemento chiave del nuovo sistema introdotto dal Regolamento: è chiamato a svolgere un ruolo di intermediazione tra gli interessi privati perseguiti dal titolare del trattamento e la volontà degli interessati a mantenere il controllo sui proprio dati[160].

Ecco perché il Garante ha fortemente consigliato la costituzione di "reti di *DPO*" come elemento fondamentale per evitare l'isolamento dei designati all'interno delle singole realtà organizzative e per confrontarsi e dialogare con chi quotidianamente affronta problematiche simili[161]. Questo tipo di pratiche renderebbe il processo di adeguamento al nuovo Regolamento più rapido e, soprattutto, costituirebbe, all'interno del meccanismo di *accountability*, un elemento a favore della *compliance* alla normativa[162].

Il tema del conflitto di interessi è stato oggetto di numerose decisioni da parte delle Autorità di controllo europee. In particolare, nel 2016 la *Bavarian Data Protection Authority* (*BayLDA*) ha rilevato un conflitto di

---

[156] *Ivi*, pp. 17 s.

[157] Cfr. MODAFFERI F., *Il regime particolare dei trattamenti dati*, cit., p. 381.

[158] *Ibidem*.

[159] *Ibidem*.

[160] *Ivi*, p. 382.

[161] *Ibidem.*

[162] *Ibidem.*

interessi in una società che aveva nominato *DPO* il proprio IT manager, il quale avrebbe in pratica dovuto controllare sé stesso[163]. Questo meccanismo di "auto-controllo"[164] non garantiva l'indipendenza richiesta al ruolo del *DPO*, il quale deve in sostanza farsi carico di quei compiti di monitoraggio che altrimenti spetterebbero alle Autorità di controllo (pur non limitando le loro possibilità di intervento)[165]. Nel caso in questione, la *BayLDA* ha informato la società di questo conflitto, chiedendo ripetutamente di provvedere alla nomina di un nuovo *DPO*; l'azienda ha però dichiarato che la nuova designazione sarebbe avvenuta nel corso di una ristrutturazione dell'organigramma allora in atto[166]. Nei mesi successivi non è però pervenuta alla *BayLDA* alcuna nota ufficiale riguardante la nomina di un nuovo *DPO*, ciò ha portato all'inflizione di un'ammenda il cui importo non è stato reso pubblico[167].

Sullo stesso tema si è pronunciata anche l'*Autorité de protection des données - Gegevensbeschermingsautoriteit* (*GBA*)[168] che nel 2020 ha imposto una sanzione pecuniaria di € 50.000 ad un'azienda di telecomunicazioni belga. In seguito ad una serie di controlli successivi ad un *data breach*, l'Autorità ha rilevato alcuni profili di non conformità al GDPR riguardo alla figura del *Data Protection Officer*[169].

In primo luogo, il *DPO* è risultato non essere coinvolto in tutti i processi concernenti i dati personali[170]; riguardo a ciò la *GBA* ha ribadito che il coinvolgimento di tale figura è "*parte fondamentale dello schema*

---

[163] Cfr. KAUFMANN J. & GUENTHER J. P., *Germany: Data Protection Officer must not have a conflict of interests*, *in Global Compliance News*, 21 novembre 2016, in https://www.globalcompliancenews.com/2016/11/21/germany-data-protection-officer-conflict-of-interest-20161121/, commento a Bayerisches Landesamt für Datenschutzaufsicht, ansbach, den 20/10/2016, in https://www.lda.bayern.de/media/pm/pm2016_08.pdf.

[164] Il termine inglese, più chiaro, è "*self-monitoring*", *ibidem*.

[165] Cfr. KAUFMANN J. & GUENTHER J. P., *Germany: Data Protection Officer must not have a conflitct of interests*, cit.

[166] V. Bayerisches Landesamt für Datenschutzaufsicht, ansbach, den 20/10/2016, testo originale in https://www.lda.bayern.de/media/pm/pm2016_08.pdf, trad. Automatica.

[167] *Ibidem.*

[168] L'Autorità di controllo del Belgio.

[169] Cfr. PANETTA R., *Gdpr, troppi Dpo in conflitto di interesse. L'outsourcing per garantire indipendenza*, in CORCOM – Corriere Comunicazioni, 13 maggio 2020, in https://www.corrierecomunicazioni.it/privacy/gdpr-troppi-dpo-in-conflitto-di-interesse-loutsourcing-per-garantire-indipendenza/, commento a Belgian Data Protection Authority, Litigation Chamber, 28/04/2020, 18, (File number: AH-2019-0013), trad. automatica in https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf.

[170] Specialmente quelli riguardanti la definizione di impostazioni predefinite in linea con il principio di *privacy by default*, *ibidem.*

operativo di valutazione delle operazioni di trattamento da parte del titolare"[171]. L'azienda si è difesa sottolineando che informare il *DPO* fosse parte integrante della propria procedura di gestione dei *data breaches* e ritenendo questa posizione sufficiente al fine di dimostrare la propria conformità al Regolamento[172].

L'Autorità belga ha invece contestato aspramente questa interpretazione, statuendo che la posizione della difesa non fosse conforme alla *ratio legis* del GDPR: infatti, riducendo il coinvolgimento del *DPO* ad una mera informazione, si priva questa figura della sua vera essenza[173]. Inoltre, la *GBA* ha evidenziato che, come parte del percorso di *accountability*, è importante coinvolgere il *DPO* fin dallo stadio primario (o comunque il prima possibile) di ogni processo concernente i dati personali e comunque di renderlo partecipe dei processi decisionali, invece di informarlo solamente[174]. È stato anche ribadito che la centralità del *DPO* non mina l'importanza del ruolo del titolare, il quale rimane la figura principale per quanto riguarda i trattamenti, determinandone modalità e fini, anche in opposizione ai pareri formulati dal *DPO*[175].

In secondo luogo, l'Autorità belga si è espressa relativamente alla posizione del *DPO* all'interno del contesto aziendale e al configurarsi di situazioni di conflitto d'interesse. Quando è stata effettuata l'ispezione, la stessa persona ricopriva il ruolo di *DPO* e contemporaneamente quello di responsabile dei dipartimenti di *Compliance*, *Risk Management* e *Internal Audit*[176].

Questo ha costituito una grave violazione dell'art. 38, par. 6, Regolamento 2016/679/UE secondo quanto rilevato dalla *GBA*, la quale ha sottolineato come il conflitto di interessi si verifichi nel momento in cui il soggetto designato come *DPO* agisca come decisore rispetto alle azioni che l'azienda può intraprendere, non solo a livello apicale, ma anche in ogni singolo dipartimento[177]. In particolare, per quanto riguarda il processo di *internal audit*, l'Autorità belga pone come discriminante per il verificarsi del conflitto di interessi il fatto

---

[171] Cfr. PANETTA R.*, Gdpr, troppi Dpo in conflitto di interesse. L'outsourcing per garantire indipendenza*, cit.

[172] Cfr. AA.VV., *The Belgian Data Protection Authority's decision 18/2020. Point of view,* in *Deloitte*, 2020, in https://www2.deloitte.com/be/en/pages/risk/articles/belgian-data-protection-authority-decision-18-2020.html, commento a Belgian Data Protection Authority, Litigation Chamber, 28/04/2020, 18, (File number: AH-2019-0013), trad. automatica in https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf, p. 6.

[173] *Ibidem.*

[174] *Ibidem.*

[175] Cfr. PANETTA R., *Gdpr, troppi Dpo in conflitto di interesse. L'outsourcing per garantire indipendenza*, cit.

[176] *Ibidem*.

[177] *Ibidem.*

che le attività svolte durante la fase di auditing siano limitate all'analisi dei processi aziendali e alla rendicontazione, oppure che queste comprendano anche la pianificazione di migliorie del sistema che possono incidere profondamente sull'approccio dell'azienda all'utilizzo dei dati[178].

Più nel dettaglio, la GBA chiarisce che il fatto che un dipartimento svolga una pura funzione di consulenza all'interno dell'azienda non è sufficiente affinché chi ricopre un ruolo di responsabilità nello stesso sia automaticamente ritenuto un mero consulente e non possa assumere, nemmeno parzialmente, le vesti di titolare[179].

La conseguenza di ciò è che il fatto che un soggetto che esercita una funzione in un qualunque dipartimento determina "*la capacità del soggetto di contribuire alla definizione delle finalità e dei mezzi del trattamento e, dunque, di assumere le funzioni tipiche del titolare*"[180]. Da ciò emerge l'idea che un responsabile di un qualsivoglia dipartimento non possa assumere contemporaneamente il ruolo di *Data Protection Officer*[181].

Inoltre, se i vertici di funzione sono in conflitto di interessi per definizione, allora la designazione di un *DPO* interno dovrebbe volgere verso soggetti in posizioni intermedie, ma qui si configurerebbe un problema in merito all'autonomia e all'indipendenza del *DPO*, con annesse complessità legate alla sua posizione nell'organigramma aziendale. In questo caso, infatti, il *DPO* si troverebbe, in caso di necessità, a porsi in contrasto con direttive aziendali provenienti da un suo superiore[182].

Per questo motivo, alcuni dei commentatori hanno proposto come soluzione al problema il ricorso a un *DPO* esterno (o "*in outsourcing*") mediante un contratto di servizi, specialmente per quelle realtà non aventi possibilità di designare un soggetto interno a tempo pieno[183].

Infine, questo provvedimento conferma l'applicabilità trasversale del principio di *accountability* su più livelli:

---

[178] Cfr. DELLI PONTI A., *Data Protection Officer interno conflitto di interessi. Commento al provvedimento del Garante Belga n.18/2020*, in *Studio legale Stefanelli.it*, 21 dicembre 2020, in https://www.studiolegalestefanelli.it/it/approfondimenti/data-protection-officer-interno-e-conflitto-interessi-provvedimento-garante-belga/.

[179] Cfr. PANETTA R., *Gdpr, troppi Dpo in conflitto di interesse. L'outsourcing per garantire indipendenza*, cit. e AA.VV., *The Belgian Data Protection Authority's decision 18/2020. Point of view,* in *Deloitte*, cit.

[180] Cfr. *ibidem* e DE CICCO D., *Conflitto di interessi del DPO, maxi multa del Garante belga ad un'azienda*, in *Cybersecurity360.it*, 8 maggio 2020, in https://www.cybersecurity360.it/legal/privacy-dati-personali/conflitto-di-interessi-del-dpo-maxi-multa-del-garante-belga-a-unazienda/.

[181] Cfr. DELLI PONTI A., *Data Protection Officer interno conflitto di interessi*, cit.

[182] Cfr. PANETTA R., *Gdpr, troppi Dpo in conflitto di interesse. L'outsourcing per garantire indipendenza*, cit.

[183] *Ibidem*.

come obbligo di dimostrarsi *compliant* sia ai principi del Regolamento (minimizzazione, liceità, ecc.), ma anche a tutti gli obblighi pratici previsti dallo stesso. In sostanza, come evidenziato nella decisione in esame, il GDPR concede, da un lato, molte libertà ai titolari in fase di implementazione del trattamento, ma richiede, dall'altro, una cospicua serie di dimostrazioni di conformità in fase di verifica[184].

3.2.5 Il ruolo del *DPO* nel Regolamento e nel sistema di accountability

Inquadrando il *Data Protection Officer* nel più generale sistema dell'accountability, si può considerare l'insieme dei suoi compiti come la generale funzione di promuovere la cultura della *data protection* all'interno dell'organizzazione di riferimento[185]. Egli contribuisce a dare attuazione agli elementi essenziali del Regolamento come i principi fondamentali del trattamento, i diritti degli interessati, gli approcci *privacy by design* e *privacy by default*, i registri delle attività di trattamento e la loro sicurezza, prendendo parte sostanzialmente ad ogni fase del trattamento[186].

Oltre a tutto questo però, non bisogna dimenticare che il Regolamento ha costituito (e costituisce ancora oggi) una modifica epocale[187] al contesto normativo precedente ed è quindi stato necessario mettere in conto un inevitabile e assai delicato periodo di attuazione progressiva delle nuove norme[188]. L'entrata in vigore del GDPR (25 maggio 2018) ha sancito l'inizio di una lunga, per certi aspetti non ancora conclusa, fase di incertezza e progressiva definizione delle nuove regole e del modo in cui esse si debbano applicare.

Si pensi poi che alcuni Stati, tra cui l'Italia[189], non hanno provveduto in tempo a adeguare la loro legislazione: il nuovo Regolamento era infatti direttamente vincolante per gli Stati membri e la sua attuazione ha reso automaticamente inapplicabili le leggi e le regole nazionali con esso incompatibili[190].

È in questo quadro così complesso che una parte della dottrina ha visto il *Data Protection Officer* come una

---

[184] Cfr. AA.VV., *The Belgian Data Protection Authority's decision 18/2020. Point of view,* in *Deloitte*, cit.

[185] Cfr. AVITABILE A., *Il data protection officer*, cit, p. 348.

[186] *Ibidem*.

[187] Cfr. RICCIO & AL., *GDPR e normativa privacy*, cit., p. 237.

[188] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali. 2, Il regolamento europeo 2016/679*, Torino, Giappichelli, 2016, pp 106 ss.

[189] Il GDPR è entrato in vigore il 25 maggio 2018, mentre la modifica al Codice privacy è stata resa effettiva solo dal 19 settembre dello stesso anno (d.lgs. 101/2018).

[190] Cfr. PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali. 2, Il regolamento europeo 2016/679*, Torino, Giappichelli, 2016, pp 108 s.

sorta di guida all'interno di questo processo di transizione, che si è protratto ben oltre il 25 maggio 2018, per le organizzazioni che trattano dati personali in grandi quantità o di tipologie particolarmente sensibili. Egli, infatti, opera, in questo senso diversamente dalle Autorità di controllo, a livello micro, costituendo una figura di raccordo tra gli interessi e le finalità dei titolari dei trattamenti, la tutela proattiva degli interessati e l'attenzione alla normativa, configurandosi quindi come un perno fondamentale del sistema di *accountability*[191].

Più in generale, il *DPO* sembra essere la figura che, nel suo doppio compito di consulenza e controllo, incorpora il vero senso dell'*accountability*. Come abbiamo visto, grazie all'approccio *privacy by design* e al principio di minimizzazione la tutela dei dati diviene parte del trattamento stesso[192].

Il Regolamento 2016/679/UE supera così l'approccio precedente della Direttiva 95/46/CE, composto da numerose prescrizioni e articolate procedure, ponendo un obiettivo che il titolare deve perseguire con la stessa intensità con cui egli si adopera per implementare i processi *core* della propria attività[193]: egli deve, cioè, garantire che la protezione dei dati avvenga non a limitazione del trattamento, ma attraverso questo.

Questo duplice scopo è racchiuso perfettamente nella figura del *Data Protection Officer*, che fin dall'inizio abbiamo presentato come una figura di consulenza, quindi di assistenza all'implementazione delle attività dell'organizzazione per quanto concerne le informazioni personali, ma anche come una figura di controllo, che vigili dove, per motivi logistici, l'Autorità garante non possa volgere lo sguardo[194].

Per questo il Regolamento, prima ancora di elencare i compiti minimi (art. 39) del *DPO*, ne descrive la posizione all'interno dell'organizzazione in cui opera, nella quale diventa uno degli attori principali della *data protection*. Forse questo elemento deve far pensare che, al di là delle mansioni specifiche, il DPO si debba vedere, specialmente nelle aziende private, come il primo portatore di una nuova cultura, concretizzando quel cambio di mentalità che anche il già citato Franco Pizzetti auspicava più di quindici anni fa[195].

---

[191] *Ibidem.*

[192] V. *supra*, cap. 2, § 2.2.2, 2.2.3.

[193] Cfr. FINOCCHIARO G., *GDPR tra novità e discontinuità: il principio di accountability*, in *Giurisprudenza Italiana*, vol. 12, 2019, p. 2777 ss.

[194] V. *supra*, cap. 3, § 3.2.4.

[195] V. PIZZETTI F., *Relazione Garante Privacy 2005*, presentata alle Camere il 7 luglio 2006, Doc-Web 1303712, in https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1303712.

Ecco che se l'*accountability* ha assunto la forma di un nuovo obiettivo, di un nuovo modo di legare la *data protection* a quelle attività che in passato si era cercato di limitare, allora il *Data Protection Officer* è da vedersi come il vettore di questa rivoluzione, non vigilando dall'esterno sui trattamenti messi in atto dalle aziende, ma penetrando all'interno dei processi di quest'ultima e diffondendo dall'interno una nuova cultura, un nuovo modo di tutelare i dati personali.

Conclusioni

Giunti alla fine di questo viaggio[1] crediamo sia doveroso volgere uno sguardo d'insieme sulle principali tappe del percorso che abbiamo seguito; tappe che hanno riguardato elementi molto eterogenei appartenenti anche a momenti storici diversi.

Siamo partiti dall'analisi di un diritto, quello alla riservatezza, antesignano della *data protection*, che si è sviluppato tra la spinta di un retaggio storico importante e la necessità di inseguire lo sviluppo delle tecnologie in grado di lederlo.

Proprio l'evoluzione tecnologica ha tradotto la prima versione della riservatezza, nell'oggi ben più noto diritto alla protezione dei dati personali, il quale si è concretizzato nella prima specifica legge per rendere manifesta l'opposizione tra due forme di governo opposte nella Germania post-bellica[2].

Negli anni '80 e '90 poi, il proliferarsi di leggi sulla *data protection* in alcuni paesi europei ha determinato una dissonanza tra le varie legislazioni nazionali, per rispondere alla quale sono intervenuti prima il Consiglio d'Europa e poi la Comunità Europa, quest'ultima con l'emanazione della Direttiva madre nel 1995.

Alla Direttiva si deve il merito di aver portato la *data protection* nella vita di tutti i giorni, ma la sua gestione del rischio ha prodotto una lunga serie di obblighi e prescrizioni aventi l'effetto di appesantire i processi delle organizzazioni che trattano i dati personali. Ciò ha contribuito a generare, specialmente nel nostro paese, un atteggiamento di avversione al tema della protezione dei dati, ritenuta per anni una noiosa serie di pratiche burocratiche.

In risposta, l'Unione Europea ha prodotto, servendosi per la verità di strumenti introdotti già dalla Direttiva come il *Working Party 29*, le Autorità di controllo e il *privacy officer*, un nuovo quadro normativo al cui centro è stato posto il principio di *accountability*.

Con l'introduzione di quello che è a tutti gli effetti un nuovo sistema, il legislatore ha superato la discrepanza tra teoria delle norme e pratica dei comportamenti, sostituendo le numerose prescrizioni della Direttiva con dei

[1] Il termine è utilizzato anche da Pizzetti nelle introduzioni e conclusioni dei volumi che abbiamo citato nel testo.

[2] V. *supra*, cap. 1, § 1.1.4.

principi generali[3] ai quali un titolare deve conformarsi determinando egli stesso, di volta in volta, le misure da adottare.

Questo cambio di sistema ha permesso un notevole snellimento delle procedure, rispondendo a un problema che era stato evidenziato dagli addetti ai lavori durante il periodo in cui era in vigore la Direttiva 95/46/CE, spostando in *ex post* l'eventuale intervento delle Autorità di controllo.

L'introduzione dell'*accountability* ha però visto la necessità di portare all'interno delle organizzazioni dei titolari una nuova cultura della *data protection* che superasse le precedenti convinzioni cui abbiamo più volte accennato e che ponesse il rispetto della normativa come uno degli obiettivi *core* delle attività.

L'intento del legislatore è stato quello di rendere la *data protection* un elemento centrale della vita aziendale, fino a rendere il fatto di implementare i trattamenti in conformità sia con le normative correnti sia con i propri interessi un vero e proprio *asset* strategico di un'azienda.

Il vettore scelto dal legislatore per questo compito è il *Data Protection Officer*, una "nuova"[4] figura professionale interna divenuta obbligatoria per le organizzazioni, pubbliche e private, che pratichino un ampio o comunque importante uso dei dati personali[5]. Il *Data Protection Officer* svolge sia la funzione di consulente per il titolare che persegue i propri obiettivi personali rispettando i principi delle normative vigenti, sia una funzione di vigilanza in prima persona sulla liceità dei trattamenti. Non solo, egli si pone come primo punto di contatto sia per gli interessati che desiderino assistenza per mantenere il controllo sui propri dati, sia per l'Autorità di controllo che voglia effettuare controlli o fornire pareri, se richiesti.

L'evidente complessità, in termini di varietà ed eterogeneità di funzioni, del compito ha portato alcuni commentatori a ritenere poco verosimile la possibilità di designare una persona singola come *Data Protection Officer*[6]. Più credibile appare invece la concezione del *DPO* come una funzione aziendale, i cui singoli compiti sono da assegnare a vari soggetti che compongono un team dedicato, anche ricorrendo a soluzioni esterne all'organizzazione mediante il contratto di servizi, strumento previsto dalla normativa stessa[7].

---

[3] V. art. 5, Regolamento 2016/679/UE.

[4] V. *supra*, cap. 3, § 3.1.

[5] V. *supra*, cap. 3, § 3.2.1.

[6] V. *supra*, cap. 3, § 3.2.3.

[7] V. art. 37, Regolamento 2016/679/UE.

Altra conseguenza della complessità del ruolo e dell'eterogeneità dei compiti a questo assegnati è il rischio del configurarsi di situazioni di conflitto di interessi, questa eventualità si accentua nelle situazioni in cui a ricoprire il ruolo in questione è un soggetto interno all'azienda.

Infatti, come statuito nella sentenza dell'Autorità di controllo belga che abbiamo analizzato[8], il ruolo di *DPO* non può essere ricoperto da nessun soggetto che disponga di potere decisionale in una qualunque altra funzione aziendale, in quanto la partecipazione alle decisioni si traduce nella concorrenza a determinare, almeno in parte, le caratteristiche del trattamento. Ne risulterebbe quindi che il soggetto decisore nominato *DPO* dovrebbe sostanzialmente controllare sé stesso, situazione apertamente in contraddizione con il GDPR.

Inoltre, secondo una parte della dottrina, anche nei casi in cui la designazione di un *DPO* vertesse su un soggetto interno non al vertice di una funzione verrebbero a generarsi alcune problematiche. Infatti, qualora fosse nominato un soggetto con tali caratteristiche, questo si troverebbe a dover vigilare circa la conformità al Regolamento di trattamenti derivanti dalle decisioni di soggetti gerarchicamente a lui superiori[9].

In sostanza, alla luce di questa decisione e dei commenti dottrinali su di essa espressi, appare chiaro che la soluzione di un *DPO* esterno si presti maggiormente a soddisfare le prescrizioni del Regolamento in materia, anche se tale scelta può essere più difficilmente intrapresa dalle organizzazioni più piccole.

La questione rimane comunque aperta a nuovi interventi specialmente da parte del legislatore, sia con veri e propri atti normativi, sia attraverso gli strumenti e gli organi, istituiti dallo stesso, che già in passato hanno contribuito a definire e perfezionare le disposizioni principali come il *Working Party 29* e le Autorità di controllo.

[8] V. *supra*, cap. 3, § 3.2.4.

[9] Cfr. PANETTA R., *Gdpr, troppi Dpo in conflitto di interesse. L'outsourcing per garantire indipendenza*, cit.

Bibliografia

AA.VV. *Come si è arrivati al GDPR: dalla privacy al Regolamento*, tratto da un intervento di PIZZETTI F. in *Privacy Lab* (Tinexta Group), blog online – 30/06/2020, con aggiornamento del 03/03/2022, in https://www.privacylab.it/IT/989/come-si-e-arrivati-al-gdpr-dalla-privacy-al-regolamento/ (consultato da ultimo il 24/05/2022).

AA.VV., *The Belgian Data Protection Authority's decision 18/2020. Point of view,* in *Deloitte*, 2020 https://www2.deloitte.com/be/en/pages/risk/articles/belgian-data-protection-authority-decision-18-2020.html (consultato da ultimo il 24/05/2022).

ATELLI M., *Il diritto alla tranquillità individuale*, Napoli, Jovene, 2001.

ALPA G. & BESSONE M. (a cura di), *Banche dati telematica e diritti della persona*, Padova, Cedam, 1984.

AULETTA T. *Riservatezza e tutela della personalità*, Milano, Giuffré, 1978.

BANTI A. M., *L'età contemporanea. Dalle rivoluzioni settecentesche all'imperialismo*, Bari, Laterza, 2009.

BERNARDI N. & AL., *Privacy officer, la figura chiave della data protection europea. Manuale operativo*, Milanofiori Assago (MI), Ipsoa, 2013.

BOLOGNINI L., PELINO E. & BISTOLFI C., *Il regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, Giuffrè, 2016.

BONGIOVANNI S., MOTTINO C., PEREGO M., *Il formulario del DPO: norme, giurisprudenza, strumenti operativi e modelli di atti,* Torino, Giappichelli, 2021.

BRANDEIS L. & WARREN S., *The right to privacy*, in *Harvard Law Review*, Vol 4 N 5 , 15/12/1890, pp 193 – 220, in https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf (consultato da ultimo il 24/05/2022).

CANCARINI S. & AL., *Data Protection Officer: guardiano od operatore della privacy? Casi pratici aziendali nei primi sei mesi di applicazione del GDPR*, in *Corporate compliance round tables 2018 (Atti del convegno)*, a cura di PICCIANO I. & BANA A., in *I quaderni del gruppo ASLA di* corporate compliance, ASLA, 2018, Cap. I, pp. 9-24, in https://www.aslaitalia.it/files/pubblicazioni/2019/ASLA%20epub%20CC2018.pdf (consultato da ultimo il 24/05/2022).

CARAVÀ E. & SCIAUDONE R., *Il codice della privacy: commento al D.Lgs. 30 giugno 2003, n. 196 e al D.Lgs 10 agosto 2018, n. 101 alla luce del Regolamento (UE) 2016/679 (GDPR)*, Pisa, Pacini Giuridica, 2019.

CATAUDELLA A., *La tutela civile della vita privata*, Milano, Giuffrè, 1972.

CAVOUKIAN A., *Privacy by Design. The 7 Foundational Principles*, in *privacybydesign.ca*, *Information of Privacy Commissioner of Ontario*, 05/2010, rev. 01/2011, in https://privacysecurityacademy.com/wp-content/uploads/2020/08/PbD-Principles-and-Mapping.pdf (consultato da ultimo il 24/05/2022).

CICCIA MESSINA A., *Responsabile della protezione dei dati*, in *Diritto e pratica del lavoro*, 2017, n. 42, pp. 2545-2548.

CILONA A., *I requisiti per la nomina del data protection officer e la certificazione lead auditor Iso 27001*, in *Media laws. Rivista di Diritto dei Media*, fasc. 1/2019, pp. 240-247, in https://www.medialaws.eu/i-requisiti-per-la-nomina-del-data-protection-officer-e-la-certificazione-lead-auditor-iso-27001/ (consultato da ultimo il 24/05/2022).

COMELLINI S., *Il responsabile della protezione dei dati (Data protection Officer-DPO)*, Santarcangelo di Romagna, Maggioli Editore, 2018.

DE CICCO D., *Conflitto di interessi del DPO, maxi multa del Garante belga ad un'azienda*, in *Cybersecurity360.it*, 8 maggio 2020, in https://www.cybersecurity360.it/legal/privacy-dati-personali/conflitto-di-interessi-del-dpo-maxi-multa-del-garante-belga-a-unazienda/ (consultato da ultimo il 24/05/2022), commento a Belgian Data Protection Authority, Litigation Chamber, 28/04/2020, 18.

DE MARTINI C., *Il diritto all'identità personale nell'esperienza operativa*, in Aa.Vv., *La lesione dell'identità personale e il danno non patrimoniale*, Milano, 1985, pp. 94 ss.

DELLI PONTI A., *Data Protection Officer interno conflitto di interessi. Commento al provvedimento del Garante Belga n.18/2020*, in *Studio legale Stefanelli.it*, 21 dicembre 2020, in https://www.studiolegalestefanelli.it/it/approfondimenti/data-protection-officer-interno-e-conflitto-interessi-provvedimento-garante-belga/ (consultato da ultimo il 24/05/2022), commento a Belgian Data Protection Authority, Litigation Chamber, 28/04/2020, 18.

DUBNICK M. J., *Accountability as Cultural Keyword*, in *Oxford Handbook of Public Accountability*, Oxford, Oxford Univrsity Press, 2014, pp. 23 – 38, in http://mjdubnick.dubnick.net/papers/2012/Dubnick%20VU%202012.pdf (consultato da ultimo il 24/05/2022).

DUBNICK M. J., *Clarifying Accountability: An Ethical Theory Framework*," in *Public Sector Ethics Finding and Implementing Value*s, Sydney, Federation Press, 1998, chapter 5, pp. 68 – 81, in http://mjdubnick.dubnick.net/pubsrw/1998/dub1998clar.html (consultato da ultimo il 24/05/2022).

ECO U., *Come si fa una tesi di laurea: le materie umanistiche*, Milano, Bompiani, 1977.

EZZAMEL M., *Accounting, control and accountability: preliminary evidence from ancient Egypt*, in *Critical perspective on accounting*, Manchester University academic press, vol. 8, 1997, pp. 563 – 601, in https://www.sciencedirect.com/sdfe/reader/pii/S1045235497901234/pdf (consultato da ultimo il 24/05/2022).

FINOCCHIARO G., *GDPR tra novità e discontinuità: il principio di accountability*, in *Giurisprudenza Italiana*, vol. 12, 2019, p. 2777 ss.

FINOCCHIARO G. & AL., *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2020.

FINOCCHIARO G., *Privacy e protezione dei dati personali: disciplina e strumenti operativi*, Torino, Zanichelli editore, 2016 (I ed. 2012).

GRECO A., *La nuova figura del data protection officer (Dpo) nell'Ue*, in *Media laws. Rivista di Diritto dei Media, fasc*. 1/2021, pp. 302-320, in https://www.medialaws.eu/rivista/la-nuova-figura-del-data-protection-officer-nellue/ (consultato da ultimo il 24/05/2022).

IASELLI M., *Fare il Data Protection Officer in Italia: un bilancio dei primi tre anni,* in *Agenda Digitale*, 28 aprile 2021, in https://www.agendadigitale.eu/sicurezza/data-protection-officer/ (consultato da ultimo il 24/05/2022).

KAUFMANN J. & GUENTHER J. P., *Germany: Data Protection Officer must not have a conflict of interests*, *in Global Compliance News*, 21 novembre 2016, in https://www.globalcompliancenews.com/2016/11/21/germany-data-protection-officer-conflict-of-interest-20161121/ (consultato da ultimo il 24/05/2022), commento a Bayerisches Landesamt für Datenschutzaufsicht, ansbach, den 20/10/2016.

KLITOU D., *Privacy-Invading Technologies and Privacy by Design*, The Hague, TMC Asser Press, 2014, in https://link.springer.com/content/pdf/10.1007%2F978-94-6265-026-8.pdf (consultato da ultimo il 24/05/2022).

LOVATI M., *Quanto sono grandi i big data?*, in *Data manager online*, 14 giugno 2018, in https://www.datamanager.it/2018/06/quanto-sono-grandi-i-big-data/ (consultato da ultimo il 24/05/2022).

LUCCHINI GUASTALLA E., *Il nuovo Regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contratto e Impresa*, vol. 34, n. 1, 2018, pp. 106-125, in https://studiolegale.leggiditalia.it/#id=10AR0000189258ART1,__m=document (consultato da ultimo il 24/05/2022).

NAPOLI S., *La figura del Data Protection Officer nel nuovo Regolamente Europeo,* in *AIEA*, Maggio 2017, in http://www.aiea.it/sites/default/files/pubblicazioni/download/la_figura_del_data_protection_officer_nel_nuovo_regolamento_europeo_0.pdf (consultato da ultimo il 24/05/2022).

OMAN S., *Implementing Data Protection in Law*, in *Scandinavian Studies in Law*, Vol. 47, 2004, pp. 389-403, in https://scandinavianlaw.se/pdf/47-18.pdf (consultato da ultimo il 24/05/2022).

PANETTA R., *Gdpr, troppi Dpo in conflitto di interesse. L'outsourcing per garantire indipendenza*, in CORCOM – Corriere Comunicazioni, 13 maggio 2020, in https://www.corrierecomunicazioni.it/privacy/gdpr-troppi-dpo-in-conflitto-di-interesse-loutsourcing-per-garantire-indipendenza/ (consultato da ultimo il 24/05/2022), commento a Belgian Data Protection Authority, Litigation Chamber, 28/04/2020, 18.

PANETTA R., IANNINI A. & ALPA G., *Circolazione e protezione dei dati personali, tra libertà e regole di mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice privacy). Scritti in memoria di Stefano Rodotà.* Milano, Giuffrè Francis Lefebvre, 2019.

PANETTA R., MAURO T., SARTORE F., *Il data protection officer tra regole e prassi*, Milano, Giuffrè Francis Lefebvre, 2021.

PISAPIA A., *La tutela multilivello garantita ai dati personali*, in *Federalismi.it*, n. 3, 31/01/2018, in https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=35666 (consultato da ultimo il 24/05/2022).

PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali. 2, Il regolamento europeo 2016/679*, Torino, Giappichelli, 2016.

PIZZETTI F. & AL., *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino, Giappichelli, 2021.

RECIO M., *Data Protection Officer: the key figure to Ensure data protection and accountability*, in *European Data Protection Law Review (EDPL)*, n. 1/2017, vol. 3, pp. 114-118, in https://edpl.lexxion.eu/ e https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/edpl3&id=118&men_tab=srchresults (consultati da ultimo il 24/05/2022).

RICCARDI J., *The German Federal Data Protection Act of 1977: Protecting the right to Privacy?*, in *Boston College International and Comparative Law Review*, Vol 6, I 1, 1983, pp. 243-271, in https://core.ac.uk/download/pdf/80399406.pdf (consultato da ultimo il 24/05/2022).

RICCIO G. M. & al., Commento all'*Art. 37 Reg. (CE) 27-04-2016, n. 2016/679/UE - Designazione del responsabile della protezione dei dati* in *Codice della Privacy commentato,* in *Commentario privacy,* in One legale by Wolters Kluwer: https://onelegale.wolterskluwer.it/document/art-37-reg-ce-27-04-2016-n-2016-679-ue-designazione-del-responsabile-della-protezione-dei-dati/9HCI0000000162?pathId=2cfef24df0e9b8.

RICCIO G. M. & al., Commento all'*Art. 38 Reg. (CE) 27-04-2016, n. 2016/679/UE - Posizione del responsabile della protezione dei dati,* in *Commentario privacy*, in One legale by Wolters Kluwer: https://onelegale.wolterskluwer.it/document/art-38-reg-ce-27-04-2016-n-2016-679-ue-posizione-del-responsabile-della-protezione-dei-dati/9HCI0000000161?pathId=22fd18d16e9318.

RICCIO G. M. & al., Commento all'*Art. 39 Reg. (CE) 27-04-2016, n. 2016/679/UE - Compiti del responsabile dei dati,* in *Commentario Privacy*, in One legale by Wolters Kluwer: https://onelegale.wolterskluwer.it/document/art-39-reg-ce-27-04-2016-n-2016-679-ue-compiti-del-responsabile-della-protezione-dei-dati/9HCI0000000198?pathId=2adcc791ca643.

RICCIO, G. M., SCORZA, G., & BELISARIO, E., *GDPR e normativa privacy. Commentato*, Milano, Wolters Kluwer, 2018.

RUFFINI GANDOLFI M. L., *Diritto alla riservatezza*, in *Digesto delle discipline privatistiche*., sez. civ., 1990, vol. VI, pp. 69-77, anche in https://onelegale.wolterskluwer.it/document/diritto-alla-riservatezza/94GI0000000334?searchId=615907269&pathId=f5a68c6b795de&offset=0#nota_11 (consultato da ultimo il 24/05/2022).

SANTAMBROGIO A., *Introduzione alla sociologia. Le teorie, i concetti, gli autori*, Roma, Laterza, 2008.

SICA S., D'ANTONIO G. & RICCIO M., *La nuova disciplina europea della privacy*, Padova, Cedam, 2016.

SORO, A., BARBAROSSA, M. & CASSANO, G., *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101,* Milano, Giuffrè Francis Lefebvre, 2018.

DE TERWANGNE, C., ROSIER K. & POULLET Y., *Le Règlement général sur la protection des données (RGPD-GDPR). Analyse approfondie*, Bruxelles, Larcier, 2018.

TONELLO F., *Democrazie a rischio. La produzione sociale dell'ignoranza*, Milano Torino, Pearson, 2019.

TORRE M., *Protezione dei dati personali, processo penale e intercettazioni*, in *Diritto penale e processo*, 2/2019, pp. 180-187, in http://hdl.handle.net/2158/1151885 e https://studiolegale.leggiditalia.it/#id=10AR0000242721ART2,__m=document (consultati da ultimo il 24/05/2022).

UHR J., *Redesigning Accountability: From Muddles to Maps*, in The Australian Quarterly, vol. 65, n. 2, pp. 1-16, in https://www.jstor.org/stable/pdf/20635716.pdf (consultati da ultimo il 24/05/2022).

ZANGHÌ C., *Istituzioni di diritto dell'Unione Europea*, Torino, Giappichelli, IV ed., 2003.

ZATTI P. & COLUSSI V., *Lineamenti di diritto privato*, Padova, Cedam, VIII ed., 2001.

ZORZI GALGANO N., *Persona e mercato dei dati: riflessioni sul GDPR*, Padova, Cedam, 2019.