UNIVERSITÀ DEGLI STUDI "MEDITERRANEA" DI REGGIO CALABRIA

DIPARTIMENTO DI GIURISPRUDENZA, ECONOMIA E SCIENZE UMANE

Dottorato di Ricerca in Giurisprudenza ed Economia

CICLO XXXII

COORDINATRICE: Prof.ssa Carmela Salazar

IL RUOLO "IBRIDO" DEL *DATA PROTECTION OFFICER* NEL REGOLAMENTO (UE) 2016/679

Tesi di dottorato della

Dott.ssa Carlotta FUSCO

Chiar.mo Prof. Attilio GORASSINI

Anno Accademico 2018/2019

ABSTRACT

Il lavoro di ricerca è incentrato su una delle principali novità introdotte dal Regolamento (UE) 679/2016: il *Data Protection Officer* (DPO), professionista specializzato in materia di protezione dei dati personali, il cui precipuo compito consiste nel coadiuvare il Titolare ed il Responsabile del trattamento nell'esercizio delle loro attività. Al fine di comprendere il rilevante ruolo giocato da tale figura professionale nel settore di riferimento, nonché la *ratio* sottesa alla previsione dello stesso, si è ritenuto necessario, in via preliminare, ricostruire l'evoluzione storica del diritto alla protezione dei dati personali, culminata il 25 maggio 2016 con l'emanazione del GDPR (acronimo di *General Data Protection Regulation*). Il GDPR tenta di offrire una risposta ai nuovi e complessi problemi causati dalla influenza sempre più pervasiva dei fenomeni tecnologici, tra cui assume particolare rilievo quello noto come "*Big Data*", che, rivoluzionando il concetto di "dato personale", ha alterato la natura stessa dei trattamenti che li riguardano. I trattamenti odierni, infatti, si caratterizzano per il fatto di esporre a rischi potenzialmente elevati il diritto alla protezione dei dati personali. Tuttavia, gli stessi devono poter essere attuati, salvo che non vi sia un potere di veto dell'Autorità pubblica, al fine di garantire ulteriori e diversi diritti, di carattere "collettivo". Pertanto, i Titolari potranno procedere al trattamento, ma con i dovuti accorgimenti. Per tale ragione, il legislatore ha imperniato l'intero sistema di tutela sul principio di *accountability* del Titolare del trattamento, in virtù del quale questi è tenuto a dare costante prova circa la conformità del suo operato ai princìpi legislativi. A tal fine, il legislatore ha previsto che il Titolare venga coadiuvato dal *Data Protection Officer*: analizzando le funzioni e le mansioni tipiche di questo professionista, che agisce nell'impresa e per l'impresa, ma che, al contempo, sembra porsi come *longa manus* dell'Autorità di controllo, verranno evidenziate alcune criticità della disciplina legislativa, che sembra non aver tenuto in debito conto le peculiarità caratterizzanti questa figura e il tipo di prestazione da questi offerta. In particolare, il dubbio che si pone è se, in considerazione delle funzioni a questi affidate, nonché del ruolo svolto, che pare possa esser ricondotto nel novero dei c.d. "ruoli sociali", sia auspicabile un ripensamento della disciplina, attraverso l'introduzione di misure idonee a garantire la massima efficacia dell'azione dello stesso, che si riflette di conseguenza sull'efficacia dell'azione del Titolare.

The research focuses on one of the main innovations introduced by the General Data Protection Regulation (hereinafter "GDPR"), the *Data Protection Officer* (hereinafter "DPO"), a key professional figure, specialized in data protection, whose primary task is to assist and consult the Controller and the Processor in their activity. To understand the key-role of this professional figure, as well as the arising needs behind its introduction, it is necessary, as a preliminary step, to reconstruct the evolution of personal data protection rights, which culminated in GDPR enactment on 25 May 2016. With the aim of offering an answer to the new, complex needs of technological phenomena, (including the one known as "*Big Data*") GDPR poses many new technical and legal measures to enforce data protection. Indeed, *Big Data* is changing the concept of "personal data" and also modalities and even the character of data processing activities.

Currently, data processing activities are characterized by the exposure of personal data to (potentially) high risks. However, these data processing activities must be able to be implemented to guarantee additional and different common rights; thus, the controller will be enabled to carry out data processing provided due precautions and protective measures are used. For this reason, the EU legislator has focused the entire new data protection legislation on the "*accountability*" principle, meaning the capacity of the controller to give proof regarding conformity of processing activities following a legislative framework.

For this reason, the controller must be assisted by the DPO. This professional figure works ***in*** the company and ***for*** the company, but, at the same time, he works like a Supervisory Authority's "*longa manus*". According to the GDPR, the DPO has duties and tasks, but, on analysing this, it will be clear how frequently it does not appear to truly take into account the professional's peculiarities and duties. The doubt arises in particular on whether, with regard to his functions and role, which seems to be included in the "social role" category, there is the need to rewrite some points of the GDPR rules, through a legislative enforcement with the introduction of other appropriate measures to ensure the best effectiveness of the controller's activities, and consequently his job effectiveness.

INDICE

CONSIDERAZIONI INTRODUTTIVE

"Diritto alla riservatezza" o "diritto alla *privacy*" e "diritto alla protezione dei dati personali" rappresentano locuzioni ormai entrate nel lessico comune di tutte le esperienze giuridiche nazionali e sovranazionali.

Spesso utilizzate in maniera sinonimica, esse in realtà sottendono situazioni giuridiche profondamente diverse, che permettono all'interprete di ricostruire lo sviluppo di questi "attributi della personalità"[1] lungo lo svolgersi del secolo XX ed i primi decenni del secolo XXI, periodi storici segnati, rispettivamente, dall'avvento dei fenomeni tecnologici e dalla sempre più pregnante pervasività degli stessi in ogni settore della vita umana, al punto da richiedere, già nella seconda metà del secolo scorso, l'intervento regolatorio del legislatore, divenuto ormai improcrastinabile, nonché, in tempi più recenti, la sua successiva revisione, segno, questo, dei rapidi mutamenti che caratterizzano l'età contemporanea.

Risale, dunque, al secolo scorso l'esigenza di adattare le forme di protezione giuridica esistenti a diritti che vedono mutare il proprio contenuto originario, nonché quella di predisporre eventuali forme di protezione di carattere innovativo, soprattutto nel caso in cui a venire in rilievo siano i diritti essenziali dell'individuo[2].

È la disciplina normativa predisposta dal legislatore a tutela delle situazioni giuridiche sopra richiamate a rappresentare, più di ogni altra, il frutto del fenomeno che ha caratterizzato la fine del secolo scorso, vale a dire quello della significativa inferenza tra evoluzione tecnologica e sviluppo delle categorie giuridiche esistenti, nonché creazione di categorie nuove.

Ma non solo: le situazioni giuridiche richiamate rappresentano, ulteriormente, il principale frutto delle influenze e delle contaminazioni tra le esperienze giuridiche dei sistemi di *civil law* e di *common law*, che avvengono sul portato della

[1] V. ZENO ZENCOVICH, *Profili negoziali degli attributi della personalità*, in *Il diritto dell'informazione e dell'informatica*, 1993, p. 545-546. L'A. motiva la preferenza per l'espressione "attributi della personalità" in luogo di "diritti della personalità" o "diritto della personalità" - a seconda dell'adesione alla teoria pluralista o monista- in quanto più idonea a rappresentare la situazione oggettiva che si intende tutelare.

[2] G. RAMACCIONI, *La protezione dei dati personali e il danno non patrimoniale. Studio sulla tutela della persona nella prospettiva risarcitoria*, Jovene editore, 2017, p. 17.

transnazionalità della rete Internet, in una declinazione che propone interrogativi inediti e pone il giurista dinanzi a sfide sempre nuove[3]. Se difatti, come si avrà modo di analizzare nel paragrafo seguente, le radici del diritto alla riservatezza vanno rintracciate nel cd. *right to privacy*, il quale nasce e si sviluppa nei confini nordamericani sul finire dell'ottocento, sarà solo con la raffinata elaborazione dottrinaria di matrice tedesca ed italiana della seconda metà del novecento che il concetto troverà una più compiuta definizione ed un inquadramento sistemico nell'ambito di quei diritti della personalità che costituiscono il frutto maturo della speculazione giuridica del secondo dopoguerra, venendone in tale contesto definiti i contorni, necessari a distinguere tale diritto da quello, differente, della protezione dei dati personali, la cui elaborazione è più recente.

È certo, inoltre, che la dimensione europea della tutela della persona e dei diritti della personalità ha avuto un'influenza oltremodo notevole sullo sviluppo di entrambi i diritti, prevalendo su quella americana, soprattutto in considerazione della maggior rilevanza progressivamente acquisita dalla persona fisica in ambito europeo, non più considerata in qualità di "consumatore" o attore del mercato, ma come soggetto con una propria dimensione esistenziale e relazionale avulsa da interessi meramente economici.

Parallelamente, come si accennava, è soprattutto lo sviluppo della tecnologia e della rete Internet negli ultimi decenni, nonché il progressivo riconoscimento del diritto di accesso come diritto della persona[4], nella dinamica dei cd. diritti nativi, a determinare non solo una evoluzione, in senso digitale, delle situazioni giuridiche esistenti, ma, ulteriormente, l'emersione di situazioni giuridiche nuove: con l'evoluzione dei sistemi di computazione informatica e con la diffusione della rete

[3] S. SICA – P. STANZIONE, *Commercio elettronico e categorie civilistiche*, Milano, 2002; E. TOSI (a cura di), *Diritto privato dell'informatica e di Internet*, Milano, 2006; G. FINOCCHIARO – F. DELFINI, *Diritto dell'Internet*, Milano, 2014; L. RUGGERI – C. PARLINGIERI, *Internet e Diritto Civile*, Napoli, 2015.

[4] Per una compiuta e attenta analisi in merito al diritto d'accesso, diritto che va a "*collocarsi nel catalogo dei cd. "diritti nativi", propri della dimensione di Internet, come diritto fondamentale, strettamente inerente alla identità ed alla realizzazione della personalità individuale, ma altresì anche alla sfera relazionale e comunicativa*" v. A. BUSACCA, *Il diritto di accesso ad Internet*, in *Ordine internazionale e diritti umani*, 2017, pp. 345-359, rinvenibile al *link* *http://www.rivistaoidu.net/content/%E2%80%9Cdiritto-di-accesso%E2%80%9D-alla-rete-internet*.

Internet, infatti, si moltiplicano i canali di comunicazione e le possibilità di scambio ed interazione tra soggetti[5].

La persona interagisce, si proietta sulla Rete, dichiara la propria identità e ne costruisce una (o più) in senso virtuale, ed in questo senso la proiezione verso l'esterno richiede una modalità di tutela diversa e più matura rispetto alla tutela difensivistica dei tradizionali diritti della personalità[6]. La prerogativa principale non è più quella di salvaguardare la propria sfera personale dalle intromissioni esterne, ma piuttosto quella di acquisire consapevolezza e poter esercitare un

[5] Sulla natura giuridica del fenomeno delle "nuove tecnologie" si rinvia all'indagine svolta da A. Gorassini. L'A., interrogandosi sulla dimensione e categoria che tale fenomeno assume, secondo la quadripartizione della fenomenologia giuridica proposta dalla scuola messinese (e dunque se occorra fare riferimento alla dimensione spaziale o a quella temporale, se alla categoria del Soggetto ovvero a quella dell'Oggetto, se ci si deve riferire ai Fatti o ai Comportamenti), attraverso un "esperimento mentale", ha escluso che le nuove tecnologie possano essere fatte rientrare nella categoria del Soggetto, o in quella dei Fatti e Comportamenti: piuttosto, sembra che le stesse possano essere ricondotte alla categoria spaziale dell'Oggetto, poiché, da un lato, l'intera infrastruttura tecnologica che garantisce la connettività a Internet si basa su elementi materiali configurabili come beni (il satellite; le stazioni terrestri chiamate NOC (acronimo di *Network Operations Center*); la parabola e un modem ad essa collegato), e, dall'altro, sono da considerare altresì beni gli algoritmi di bit che vengono trasferiti mediante tali strumento. Spiega l'A. che "*anche se fossero solo espressione di energia, in Italia esiste l'art. 814 c.c. («si considerano beni mobili le energie naturali che hanno valore economico»); e anche se si potessero avere dubbi sulla naturalità dell'energia dei bit, essendo essi senz'altro possibile oggetto di diritti, sarei comunque coperto dal portato normativo dell'ultimo inciso dell'art. 813 c.c. («le disposizioni concernenti i beni mobili si applicano a tutti gli altri diritti»)*". La tecnologia, inoltre, proprio in ragione dell'energia che la governa, non solo occupa uno spazio, ma ne crea altro, scaricando altrove l'entropia della sua creazione, in gran parte delocalizzandola nello spazio siderale, realtà possibile proprio per una sovrapposizione di stati dell'energia. Tali considerazioni incidono, rendendola complessa, sull'indagine di questa realtà giuridica rilevante, se guardata dalla prospettiva dell'oggetto. Come spiega l'Autore, infatti, "*se guardo lo spazio occupato nel mondo reale conosciuto e percepito, dal punto di vista della fenomenologia giuridica ho un bene transnazionale sostanzialmente immobile (nodi, reti e quant'altro perché incorporati al suolo) da qualificare. Se guardo alla potenza e contenuto temporale, anche sotto il profilo del calore, del bit, trovo la struttura un bene mobile posto tra energia e cosa che incorpora valore, da definire per l'appropriazione. Se guardo alla dimensione unitaria spazio/tempo, l'entropia creata dalla tecnologia (ma essa stessa per la funzione d'onda e il suo collassare) diventa spazio siderale Rete Internet*". Proprio alla luce di tali considerazioni, appare evidente come il concetto di "dominio" vede oggi trasformata la propria natura, da ciò derivando la necessità per il sistema di riqualificare tale concetto giuridico; e da esso verificare e riposizionare la situazione di fatto che identifica il possesso, anche in considerazione del fatto che molte "cose tecnologiche" possono oggi essere incorporate e divenire cose inerenti il Soggetto. Inoltre, proprio il Soggetto produce delle informazioni che valgono come Bene o come Rifiuto, nel mondo spaziale in cui si svolge la sua vita; e se sono Bene, è possibile che l'Altro tragga beneficio dal loro sfruttamento come cose, venendosi a creare così un momento di conflitto da gestire mediante il diritto. V. A. GORASSINI, *Lo spazio digitale come oggetto di un diritto reale?*, in *Medialaws*, 02/2018, Giugno, pp. 53 ss.

[6] Scrive al riguardo R. Messinetti che "*il potere di controllare la propria identità è il nucleo della tutela della persona umana nella c.d. società dell'informazione della contemporaneità; uno strumento necessario per preservarne le libertà (in primis, autodeterminarsi) nel tempo della c.d. sorveglianza globale e della digitalizzazione del mondo*". V. R. MESSINETTI, *La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, in *Contratto e Impresa*, 2019, 861-862.

controllo sui propri dati e sulla circolazione degli stessi nell'ecosistema Internet, indicato dalla dottrina come "alla ricerca di regole"[7].

Su queste premesse, si deve prendere atto dell'esistenza di una sorta di sequenza non solo temporale, ma anche logica, tra "diritto alla riservatezza" (*right to privacy*) inteso come diritto introflesso ed indirizzato alla tutela della sfera personale, e "diritto alla protezione dei dati personali" da intendersi come diritto estroflesso, teso alla tutela delle informazioni e della identità digitale, costituita dalle molte tracce che la persona dissemina, consapevolmente o inconsapevolmente, nella Rete[8]. La dimensione intimistica e la natura difensivistica della tutela di matrice novecentesca del diritto alla riservatezza (che si manifesta a pieno negli artt. 10 ed 11 del codice civile e nell'impianto della Legge n. 633/1941 sul diritto d'autore), del resto, non appare più confacente e sufficiente ad una dimensione che dilata tempi e modalità della circuitazione, chiamando in causa una pluralità di soggetti, coinvolti a vario titolo nelle attività che concernono i dati personali e che, grazie allo sviluppo tecnologico, permettono di realizzare sempre nuove attività, arrivando finanche alla decostruzione e ricostruzione di blocchi di dati.

Ancora, la dimensione spiccatamente privatistica sembra dover cedere il passo ad una diversa considerazione, nella quale all'interesse del singolo si affianca e si sovrappone l'interesse della comunità, ascrivendo la tutela dei dati personali ad un catalogo di diritti sociali, proiettati al bene comune ed al benessere degli individui, da ciò derivando una evoluzione in senso pubblicistico della tutela delle situazioni coinvolte, resa possibile in virtù dei contenuti della normativa di derivazione europea e delle norme delle Carte Fondamentali dell'UE.

---

[7] P. PASSAGLIA – D. POLETTI, *Nodi virtuali legami informali: internet alla ricerca di regole*, *Pisa Univesity Press*, 2017. Proprio il problema della regolamentazione della rete Internet costituisce il punto di emersione delle criticità dell'intero sistema, e ciò per varie ragioni, che vengono individuate dagli autori nell'inedita dimensione a-spaziale ed a-temporale caratterizzante la Rete, che sembra porre in crisi le coordinate di riferimento della norma giuridica; nella natura transnazionale, che supera la tradizione del localismo giuridico; nell'aspirazione alla autoregolamentazione, che mal tollera, da parte di diversi esponenti della dottrina ed operatori della Rete, l'idea di una regolamentazione statale etero-imposta; nel continuo ed inarrestabile sviluppo della realtà digitale e delle modalità di comunicazione, che pongono nuove modalità nel rapporto uomo-macchina.

[8] R. MESSINETTI, op. cit.; E. TOSI, *Privacy digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo Codice della Privacy*, in E. TOSI (a cura di) *Privacy digitale*, Giuffrè, 2019, p. 1; G. PASCUZZI, *Il diritto dell'era digitale*, Il Mulino, 2016.

In questo senso, proprio seguendo la dimensione europea del diritto alla protezione dei dati personali, che si sviluppa in chiave normativa prendendo le mosse da esperienze maturate nei singoli ordinamenti, per giungere ad una sintesi che aspira ad essere sistema, un momento di fondamentale importanza può considerarsi la Carta dei diritti fondamentali dell'Unione europea, proclamata, quasi che anche la data assuma una simbologia precisa, il 7 dicembre del 2000 dal Parlamento europeo, dal Consiglio e dalla Commissione Europea[9]. La Carta sembra costituire uno spartiacque tra una considerazione più statica quale quella che emerge dalla Direttiva 95/46/CE[10] ed una considerazione necessariamente più dinamica, che porterà, nel 2016, all'emanazione del Regolamento europeo sulla protezione dei dati personali[11].

Si apriva così il nuovo millennio in Europa: a distanza di cinquant'anni dall'emanazione della Convenzione Europea dei Diritti dell'Uomo (CEDU), preso atto dell'evolversi della realtà sociale e dell'affermarsi di un nuovo assetto di diritti fondamentali della persona, tra cui in particolare i diritti della personalità[12], l'Unione Europea, garante dei "valori indivisibili e universali di dignità umana, di libertà, di uguaglianza e di solidarietà", si impegnava a "rafforzare" la tutela di quei "nuovi" diritti, frutto dell'evoluzione "della società, del progresso sociale e degli sviluppi scientifici e tecnologici"[13]. Tale rafforzamento non poteva che

[9] La Carta, anche nota come "Carta di Nizza", è stata successivamente oggetto di numerose modifiche, tanto da essere nuovamente proclamata il 12 dicembre 2007. La stessa, pur non essendo vincolante in un primo momento, è divenuta fonte vincolante per gli Stati membri a far data dal 2009, anno in cui venne adottato il Trattato di Lisbona. Il TUE, all'articolo 6, paragrafo 1, ha previsto infatti che a questa venisse riconosciuto lo stesso valore giuridico dei trattati europei.

[10] Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

[11] Regolamento (UE) 2016/679 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.

[12] È vasta la letteratura esistente in materia di diritti della personalità. Senza pretesa di esaustività, si rinvia a A. DE CUPIS*, I diritti della personalità*, in F. MESSINEO – L. MENGONI*, Trattato di diritto civile e commerciale*, IV, Milano, 1982; D. MESSINETTI, voce *Personalità (diritto della)*, in Enc. dir., XXXIII, Milano, 1983; V. ZENO-ZENCOVICH, P*ersonalità (diritti della)*, in N. LIPARI – P. RESCIGNO (a cura di), *Diritto civile*, Milano, 2009, I, p. 495 ss.; G. ALPA, *I diritti della personalità*, in G. ALPA – G. RESTA, *Le persone e la famiglia. 1) Le persone fisiche e i diritti della personalità*, in R. SACCO, *Trattato di diritto civile*, Torino, 2006.

[13] Nel preambolo della Carta si legge "*Consapevole del suo patrimonio spirituale e morale, l'Unione si fonda sui valori indivisibili e universali di dignità umana, di libertà, di uguaglianza e di solidarietà; l'Unione si basa sui principi di democrazia e dello stato di diritto. Essa pone la persona al centro della sua azione istituendo la cittadinanza dell'Unione e creando uno spazio di libertà, sicurezza e giustizia. L'Unione contribuisce al mantenimento e allo sviluppo di questi*

essere attuato mediante l'emanazione di un nuovo testo giuridico, che sarebbe sì divenuto vincolante in un momento successivo[14], ma che assumeva una rilevanza notevole già al tempo della sua entrata in vigore, per il solo fatto di sancire per la prima volta, in maniera visibile, il carattere fondamentale e la portata dei diritti umani "di nuova generazione" dei cittadini dell'Unione, raccogliendo in un testo organico le tre categorie dei diritti civili e politici, dei diritti economici e sociali e dei diritti del cittadino europeo[15].

Il ruolo giocato dalla Carta appare, dunque, estremamente rilevante. La stessa, infatti, costituisce un'occasione, per il legislatore, di aggiornamento del catalogo dei diritti emersi nella seconda metà del secolo precedente[16], che diventano oggetto di un processo di cd. "costituzionalizzazione"[17]. Tra questi, emerge in particolare quello relativo alla protezione dei dati personali, che diviene oggetto di

---

valori comuni, nel rispetto della diversità delle culture e delle tradizioni dei popoli europei, dell'identità nazionale degli Stati membri e dell'ordinamento dei loro pubblici poteri a livello nazionale, regionale e locale; essa cerca di promuovere uno sviluppo equilibrato e sostenibile e assicura la libera circolazione delle persone, dei beni, dei servizi e dei capitali nonché la libertà di stabilimento. A tal fine è necessario, rendendoli più visibili in una Carta, rafforzare la tutela dei diritti fondamentali alla luce dell'evoluzione della società, del progresso sociale e degli sviluppi scientifici e tecnologici. La presente Carta riafferma, nel rispetto delle competenze e dei compiti della Comunità e dell'Unione e del principio di sussidiarietà, i diritti derivanti in particolare dalle tradizioni costituzionali e dagli obblighi internazionali comuni agli Stati membri, dal trattato sull'Unione europea e dai trattati comunitari, dalla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, dalle carte sociali adottate dalla Comunità e dal Consiglio d'Europa, nonché i diritti riconosciuti dalla giurisprudenza della Corte di giustizia delle Comunità europee e da quella della Corte europea dei diritti dell'uomo. Il godimento di questi diritti fa sorgere responsabilità e doveri nei confronti degli altri come pure della comunità umana e delle generazioni future".

[14] Si rinvia al par. 2.4.

[15] A. BRECCIA, *Riconoscimento e politica dei diritti umani sul piano europeo e internazionale*, in L. PANELLA (a cura di), *I diritti umani nella giurisprudenza e nella prassi del diritto internazionale ed europeo*, Giappichelli, 2013.

[16] Si usa definire i diritti riconosciuti dalla Carta di Nizza quali "nuovi diritti". A tal riguardo, Stefano Rodotà ha evidenziato che "*un'espressione come "nuovi diritti" dev'essere considerata, a un tempo, accattivante e ambigua. Ci seduce con la promessa di una dimensione dei diritti sempre capace di rinnovarsi, di incontrare in ogni momento una realtà in continuo movimento. Al tempo stesso, però, lascia intravedere una contrapposizione tra diritti vecchi e diritti nuovi, come se il tempo dovesse consumare quelli più lontani, lasciando poi il campo libero ad un prodotto più aggiornato e scintillante. Si parla di "generazioni" dei diritti, e questa terminologia, identica a quella in uso nel mondo dei computer potrebbe indurre a ritenere che ogni nuova generazione di strumenti condanna all'obsolescenza e all'abbandono definitivo tutte le precedenti. Ma il mondo dei diritti vive di accumulazione, non di sostituzioni...*", v. S. RODOTA', *I nuovi diritti che hanno cambiato il mondo (Stralcio dell'intervento alle "Lezioni Norberto Bobbio" - Torino 25/10/2004)*, rinvenibile al *link* http://www.privacy.it/archivio/rodo20041026.html.

[17] R. LATTANZI, *«Diritto alla protezione dei dati di carattere personale»: appunti di viaggio*, in AA. VV., *Diritto alla privacy e trattamento automatizzato dei dati fra diritto civile, diritto penale e diritto internazionale ed europeo*, *I quaderni europei*, Aprile 2014 n. 63, p. 11.

regolamentazione specifica nell'art. 8 della Carta[18], a dimostrazione del rilievo acquisito dallo stesso nell'ambito della categoria dei diritti della personalità[19], e, ulteriormente, della necessità, profondamente avvertita alla fine del XX secolo, di individuare il crinale di distinzione tra tutela dei dati personali e diritto alla riservatezza. Quest'ultimo, declinato nella Carta di Nizza come "diritto al rispetto della vita privata e familiare"[20], al contrario del diritto alla protezione dei dati personali, era già stato riconosciuto come diritto fondamentale, a livello europeo, per mezzo della Convenzione Europea dei Diritti dell'Uomo[21], la quale, si ricorda, era stata approvata ben cinquant'anni prima. Con la Carta di Nizza si giunge, dunque, alla piena diversificazione dei due diritti: in tal senso, non deve trarre in inganno l'uso polisemantico, spesso confuso e confusionale, che in quegli anni (ed ancora oggi) veniva fatto del termine "*privacy*" [22], per riferirsi ad entrambi i concetti di protezione e riservatezza, a fronte della opportuna diversificazione delle due figure. Sebbene, infatti, il diritto alla protezione dei dati personali fosse comunque stato oggetto di attenzione da parte del legislatore europeo già in epoca antecedente alla Carta di Nizza – e prova ne sono i numerosi atti normativi

[18] Carta di Nizza, art.8: "*1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 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*."

[19] Oltre al compimento del processo di costituzionalizzazione, è stato affermato che con la Carta di Nizza si è giunti anche al termine del processo di autonomizzazione del diritto alla protezione dei dati personali rispetto ad altre differenti situazioni giuridiche soggettive. V. R. LATTANZI, op. cit., p. 11.

[20] Carta di Nizza, art. 7: "*Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni*".

[21] CEDU, art. 8: "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. 3. Il rispetto di tali regole Ł soggetto al controllo di un'autorità indipendente*".

[22] Scrive G. Finocchiaro "*Il termine privacy, comunque lo si pronunci, è oramai polisenso e indica una molteplicità di beni giuridici e di interessi suscettibili di differente tutela. Innanzitutto, il bene della riservatezza in senso stretto, cioè la tutela della vita privata. La segretezza, in alcuni casi. La privatezza dello spazio, in altri. La protezione delle informazioni (c.d. informational privacy), in altri ancora*." in G. FINOCCHIARO, *Riflessioni sul poliedrico Regolamento europeo sulla privacy*, in *Quaderni costituzionali*, Fascicolo 4, dicembre 2018, p. 895.

adottati al fine di dettarne una disciplina quanto più compiuta possibile[23] - lo stesso non veniva ancora considerato alla stregua di diritto fondamentale[24], al contrario del diritto alla riservatezza, che, come già evidenziato, può considerarsi il suo antecedente logico e cronologico. Sul punto deve osservarsi come la maggior parte dei provvedimenti normativi adottati prima del 2000 configurino e regolino un diritto alla protezione dei dati indirizzato e funzionalizzato alle esigenze del mercato, non rivolto alla dimensione esistenziale della persona, quanto piuttosto ad un suo agire in un preciso contesto di matrice economica.

Il mutamento di prospettiva che si avvia con la Carta di Nizza, e che determina la lunga riflessione che porterà, nel 2016, al Regolamento europeo, appare sequenziale proprio al mutato clima che caratterizza il rapporto tra "area di mercato" ed "area di non-mercato" della Rete: con l'assurgere della persona a baricentro del sistema, e con una maggiore attenzione ai profili attinenti la sfera della personalità, si registra una sorta di emancipazione della tutela dei dati personali che, da situazione strumentale al mercato, assurge a situazione autonoma, capace di proporsi nel catalogo dei diritti fondamentali e di rivendicare così la necessità di un adeguato apparato di strumenti rimediali in caso di violazione o di condotta antigiuridica.

Proprio sugli strumenti rimediali appaiono opportune alcune considerazioni, che verranno meglio approfondite nel corso dell'elaborato, dal momento che sia la cd. "costituzionalizzazione" del diritto, che la sua qualificazione in termini di diritto

[23] Tra questi assumono preminente rilievo la Direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati; la Direttiva 97/66/CE sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni; a livello internazionale si ricorda poi la Convenzione n. 108 del 28 gennaio 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale.

[24] Nelle Spiegazioni allegate alla Carta si è sostenuto che l'articolo 8 della Carta di Nizza si fonda sull'art. 286 del Trattato CE (così come modificato dal Trattato di Maastricht nel 1997), sulla Direttiva 95/46/CE, nonché sull'art. 8 della CEDU e sulla convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di caratteri personali n. 108 del 28 gennaio 1981, lasciando implicitamente sottendere che lo stesso non presenta il portato innovativo che si suole spesso attribuirgli. Tuttavia, non sembra potersi condividere la lettura restrittiva operata dal legislatore europeo, in quanto "*il margine di innovazione dell'art. 8 è piuttosto significativo. E non consiste soltanto nel "costituzionalizzare" il diritto alla protezione dei dati personali, ma anche, e forse specialmente, nell'emancipare definitivamente quest'ultimo da quella connessione alla dimensione economica propria del consolidamento del mercato interno che invece caratterizzava, almeno ab origine, il portato normativo della direttiva 95/46/CE*". V. O. Pollicino, *Un digital right to privavy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain*, in *Dir. Inf.*, 2014, p. 572.

fondamentale, sembrerebbero richiedere la predisposizione di strumenti in grado di assicurare una tutela multilivello, di carattere sia pubblicistico, con ciò riferendosi, in particolare, al controllo esercitato dall'Autorità pubblica di controllo, sia privatistico, con ciò riferendosi agli obblighi gravanti sul titolare del trattamento.

In questo senso, l'evoluzione segnata dal passaggio dalla Direttiva 95/46/CE al Regolamento 2016/679, passando attraverso l'emanazione della Carta di Nizza, sembra caratterizzata dalla costante ricerca di un miglioramento quantitativo e qualitativo degli strumenti rimediali, con un andamento che si sviluppa in parallelo alla complessità del sistema e segna il suo punto di arrivo (attuale) con l'introduzione della figura del *Data Protection Officer* (DPO), professionista nell'impresa e per l'impresa ma che, per diversi aspetti, sembra porsi, altresì, come ombra dell'Autorità di controllo. Si è scritto "introduzione", anche se sarebbe più adeguato parlare di "generalizzazione", dal momento che, ben prima del 2016 (anno di emanazione del Regolamento), la figura era già nota nell'ordinamento tedesco ed in quelli di diversi paesi dell'area mitteleuropea, potendo inoltre già rintracciarsi un suo antecedente nella figura del *Data Protection Official*, istituita dalla Direttiva 95/46/CE. Tuttavia, la scelta del legislatore europeo di regolare a sistema la figura ed i compiti di questo professionista della *privacy* digitale, non può e non deve liquidarsi con una semplice considerazione sulla preponderanza del diritto tedesco in chiave europea, quanto piuttosto deve essere valutata nell'ottica di quella duplice funzione di tutela degli interessi dei soggetti coinvolti, a diverso titolo, nelle attività di circolazione e trattamento dei dati e, parallelamente, di tutela dell'interesse alla corretta circolazione dei dati ed al rispetto delle situazioni giuridiche implicate.

Pertanto, dopo aver ripercorso, nel primo capitolo, attraverso un'analisi retrospettiva, i momenti più significativi dell'itinerario normativo che ha caratterizzato il diritto alla protezione dei dati personali (al fine di meglio inquadrare la fattispecie oggetto di studio), e dopo aver analizzato, nel secondo, lo scenario normativo attuale cristallizzato nel GDPR, mettendone in luce i profili più significativi ed innovativi, nel terzo e quarto capitolo ci si concentrerà in via esclusiva sull'analisi della nuova figura del DPO, come rappresentata nel GDPR

ed attuata nell'ordinamento italiano, cercando di ricostruirne non soltanto i requisiti e le diverse funzioni in rapporto alle attività di trattamento ed alla realizzazione del principio di *accountability* nell'impresa, ma evidenziando altresì quelle funzioni che, rapportate alla tutela dell'interesse generale rispetto al corretto trattamento dei dati, mettono in luce le criticità di un sistema che sembra non aver tenuto in debita considerazione le peculiarità di questa "nuova" figura e la crescente complessità delle attività di trattamento dei dati, delineando un quadro di responsabilità incentrato sul titolare, e perciò ponendo l'interrogativo sulla necessità di una parziale revisione della disciplina normativa.

CAPITOLO PRIMO

L'EVOLUZIONE DEL DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI: DAL DIRITTO ALLA PRIVACY STATUNITENSE ALLA DIRETTIVA 95/46/CE

1. Il diritto alla protezione dei dati personali come evoluzione del concetto di *privacy*

Protezione dei dati personali, tutela della riservatezza, salvaguardia della vita privata e familiare, sono tutte espressioni che, direttamente o indirettamente, rimandano ad uno dei temi più dibattuti del nuovo millennio, quello della *privacy*, termine comunemente utilizzato per fare riferimento, appunto, a tutto ciò che attiene la complessa disciplina della protezione dei dati personali[25]. Il concetto in esame, come già evidenziato da autorevole dottrina, rappresenta una conquista delle società progredite, costituendo l'espressione più evidente di tutto ciò che è incontrovertibilmente legato al progresso tecnologico che ha interessato tali società nel secolo precedente, dapprima quelle statunitensi ed a seguire le altre[26].

[25] V. CUFFARO*, Il diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia: elementi per un bilancio ventennale*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, *I dati personali nel diritto europeo*, Giappichelli editore, 2019, p. 4.

[26] R. Pardolesi scrive "*il diritto alla privacy è una conquista recente delle società "progredite" che, offrendo modelli di vita intensi – spesso accompagnati da momenti di esagitata ricerca di (o esposizione a) pubblicità -, suscitano un forte bisogno di ritrovarsi alle prese con sé stessi. […] L'esigenza della privacy è sentita nelle comunità economicamente avanzate, che permettono e favoriscono occasioni di incontro, profili professionali esposti all'attenzione della collettività, comunicazioni di massa, raccolte di dati e via dicendo; in queste condizioni, inimmaginabili in una società rurale, il bisogno di mantenere riservate le vicende private ovvero di controllare la circolazione di dati personali si fa impellente"*. V. R. PARDOLESI, *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*", in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè, 2003. Cfr. anche S. Rodotà, che rileva "*la nascita della privacy può essere riportata al disgregarsi della società feudale, nella quale gli individui erano tutti legati da una complessa serie di relazioni, che si riflettevano nell'organizzazione stessa della loro vita quotidiana: l'isolamento era privilegio di pochissimi eletti o di coloro i quali, per necessità o scelta, vivevano lontani dalla comunità -mistici o monaci, pastori o banditi. Questa possibilità, poi, si estende a quanti dispongono dei mezzi materiali che consentono di riprodurre, anche nell'ambiente urbano, condizioni tali da appagare il nuovo bisogno di intimità: e questo è un processo nel quale intervengono diversi fattori, dalle nuove tecniche di costruzione delle abitazioni alla separazione tra luogo in cui si vive e luogo di lavoro (la casa "privata" contrapposta all'ufficio). La privacy si configura come una possibilità che la borghesia riesce a realizzare grazie alle trasformazioni socio-economiche determinate dalla rivoluzione industriale. Sono, infatti, proprio le condizioni materiali di vita ad escludere la privacy dall'orizzonte della classe operaia*" in S. RODOTA', *Repertorio di fine secolo*, Laterza editori, 1999, p. 205.

Nato negli Stati Uniti al termine degli anni '80 del secolo XIX, grazie al noto saggio dei giuristi Samuel D. Warren e Louis D. Brandeis[27], e declinato inizialmente come estensione del diritto di proprietà fondiaria – nello specifico, come diritto a non subire ingerenze nella propria sfera privata, intesa non più e non soltanto in senso fisico, coincidente col concetto di abitazione (il già noto *ius excludendi alios*), ma come estensione dei concetti di autonomia e dignità dell'individuo (*right to be let alone*)[28], si è assistito nel tempo ad un mutamento della sua concezione originaria, tanto che a tale significante sono ancora oggi riconducibili, come si anticipava in premessa, diversi significati, a volte anche contrastanti fra loro[29] .

Una delle prime occasioni in cui emerge questa nuova considerazione del diritto alla *privacy* è da rintracciarsi nel caso *Griswald v. Connecticut*, datato 1965[30]: nella sentenza in esame, la Corte Suprema statunitense ha offerto una reinterpretazione del concetto, svincolandolo dal diritto di proprietà e definendolo quale "*espressione del principio di libertà e di autodeterminazione personale*", riconoscendone, per la prima volta, il suo fondamento costituzionale. Tale lettura interpretativa, oggetto di sviluppi vertiginosi negli anni successivi, ha fatto sì che la dottrina americana riconducesse a questo diritto non più e non soltanto la possibilità per l'individuo di vietare le interferenze nella propria sfera privata, ma altresì quella di controllare l'uso che altri facciano dei propri dati, una volta che

---

[27] S. D. WARREN, L. D. BRANDEIS, *The right to privacy*, *Harvard Law Review*, Vol. 4, No. 5 (Dec 15, 1890), pp. 193-220.

[28] Gli autori, prendendo atto delle nuove tecniche di invasione della sfera privata (nel saggio si faceva riferimento in particolare alla fotografia, in quanto uno dei due, Warren, avvocato bostoniano che conduceva una vita mondana particolarmente lussuosa, aveva attirato l'attenzione dei giornali scandalistici, che continuavano a pubblicare le foto delle feste organizzate nella sua villa), affermavano la necessità che la legge garantisse non più e non solo il diritto a non subire invasioni della proprietà intesa in senso fisico, ma anche di quella relativa alla propria persona. In sostanza, viene "*superata l'idea "proprietaria" della privacy, per approdare ad una visione della tutela della vita privata strettamente correlata alla dimensione personalistica dell'individuo*". V. A. MANTELERO, *Il costo della privacy tra valore della persona e ragione d'impresa*, Giuffrè, Milano, 2007. In merito alle vicende in questione scrive anche U. Pagallo "*come ben presto avrebbe scoperto a proprie spese la famiglia Brandeis, oggetto di un antesignano scandalo giornalistico, la circolazione abusiva di immagini personali, per la prima volta sfruttabile quasi in tempo reale su scala industriale, era destinata a produrre un mix micidiale d'interessi commerciali ed economici, tra l'interesse morboso della populace e l'esigenza di una "nuova riservatezza*" *cui il common law doveva provvedere con adeguati mezzi di tutela*". V. U. PAGALLO*, La tutela della privacy negli Stati Uniti d'America e in Europa*, Giuffrè, 2008, p. 7.

[29] A. MONTI, *Tutela della vita privata, protezione dei dati personali e privacy. Ambiguità semantiche e problemi definitori*, in *Diritto di internet*, 1/2019.

[30] *Griswold v. Connecticut 381 U.S. 479 (1965)*.

gli stessi siano usciti fuori dal proprio controllo. Questa nuova dimensione della *privacy* rappresenterà un modello di svolta per il dibattito sul tema, in quanto, da una dimensione di carattere preminentemente individuale, sintetizzata nell'espressione "*right to be let alone*", si passa ad una più marcatamente sociale, in cui diventa centrale il modo in cui l'individuo sviluppa la propria personalità attraverso la relazione con gli altri[31].

Ed è proprio nel momento in cui, nel suo territorio d'origine, il concetto di *privacy* vede stravolto il suo significato originario, che lo stesso viene importato entro i confini europei[32], per riferirlo non tanto, o meglio non solo, al diritto alla riservatezza, inteso come diritto a impedire la circolazione delle notizie personali, quanto, piuttosto, al diverso, e più nuovo, diritto alla protezione dei dati personali. Al termine del XX secolo, infatti, la *privacy* in Europa, intesa nel senso di riservatezza, o meglio rispetto della propria vita privata, si andava evolvendo "adattandosi alle esigenze concrete della società europea e, nello specifico, prediligendo un'accezione strettamente correlata ai nuovi strumenti di comunicazione – quali la televisione e mass media – ed informatici – quali i computer, i telefoni mobili e così via –.

In Europa, dunque, la *privacy* è principalmente intesa come – sinonimo di – tutela dei dati personali"[33]. Alcuni autori hanno sostenuto, in tal senso, che proprio la protezione dei dati personali costituisce una versione, in termini di "esternalità" europea, di quell'evoluzione del concetto di *privacy* avvenuta nel diritto statunitense[34], sebbene i due concetti non possano ritenersi perfettamente sovrapponibili, poiché il diritto alla protezione dei dati personali, come già

[31] G. RAMACCIONI, op. cit., p. 67.

[32] Tra i primi contributi in merito, occorre segnalare S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973; R. PARDOLESI, *Riservatezza: problemi e prospettive*, in M. SPINELLI (a cura di), *Responsabilità civile*, vol. II, Bari, 1974, p. 310, p. 316 ss. e p. 378 ss.; A. BALDASSARRE, *Privacy e Costituzione. L'esperienza statunitense*, Roma, 1974, A. BELVEDERE, *Riservatezza e strumenti d'informazione*, in N. IRTI (a cura di), *Dizionari di diritto privato*, vol. 1, Diritto civile, Milano, 1980.

[33] A. FABBRICOTTI, L. RAPONI, *La struttura multilivello della protezione dei dati personali in Europa*, in *Rivista italiana per le scienze giuridiche*, 8/2017, pp. 395 ss.

[34] S. CALZOLAIO, *Protezione dei dati personali*, in «*Dig. Disc. Pubbl.*», Agg., Utet Giuridica - Wolters Kluwer, 2017, p. 594-635.

evidenziato, rappresenta solo uno specifico ambito di esercizio della *privacy* statunitense[35].

Il concetto di *privacy* si afferma, dunque, nel panorama europeo, con rinnovata forza, e ivi si impone anche e soprattutto in conseguenza dello sviluppo e della crescente diffusione delle nuove tecnologie. A cominciare dalla diffusione di banche dati sempre più massicce e potenti, tanto nel settore pubblico quanto in quello privato[36], passando attraverso i mezzi di comunicazione di massa (dapprima la stampa giornalistica, poi la televisione), e avanzando storicamente sino alla diffusione della rete Internet nei primi anni Settanta, si è assistito sempre di più ad un mutamento di prospettiva importante: si tratta, infatti, di un'evoluzione che ha portato al centro dell'attenzione non solo quelle informazioni private relative a un esiguo numero di individui, aventi interesse di cronaca, ma tutte quelle informazioni che, anche se singolarmente irrilevanti, riguardano ogni individuo, e che vengono costantemente messe in circolazione grazie alle nuove tecnologie[37]. Com'è stato già autorevolmente rilevato da S. Rodotà "siamo di fronte alla possibilità di tali e tante forme di trattamento elettronico delle informazioni personali che vengono radicalmente rimessi in discussione lo stesso sviluppo della personalità, le forme delle relazioni personali e sociali"[38].

L'individuo, in tal modo, sembra perdere il controllo sui propri dati, che non sempre vengono comunicati e ceduti volontariamente, ma che spesso vengono carpiti senza che questi ne sia a conoscenza (date le innumerevoli "tracce" disseminate quotidianamente, non solo *online*), oppure devono necessariamente essere ceduti al fine di usufruire di un servizio di cui altrimenti non si potrebbe

---

[35] J. Q. WITHMAN, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, in Yale Law Journal, 2004, vol. 113, n. 1, 1151-1221.

[36] Non ci si trova più dinanzi a banche dati cartacee, bensì a banche dati digitali, esito della informatizzazione dei pre-esistenti archivi cartacei: "*con la digitalizzazione delle informazioni si ha invece la possibilità di mettere insieme le diverse tessere che compongono il mosaico dell'identità individuale, nonché diviene agevole ricercare le connessioni esistenti fra individui sula base di dati comuni, cosa che in passato poteva essere realizzata solo con grande dispendio di tempo, mediante l'accesso a vari archivi, non di rado distribuiti in luoghi diversi sul territorio*". V. A. MANTELERO, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati*, in G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, 2017, p. 287.

[37] V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia*, op. cit., p. 7.

[38] S. RODOTA', *Repertorio di fine secolo*, *op. cit.*, p. 202.

godere. Ma il problema non è limitato esclusivamente alla "cessione", volontaria o meno, di informazioni a terzi, titolari delle attività di trattamento, bensì anche alla capacità di questi ultimi di raggiungere obiettivi che talvolta superano gli scopi originariamente perseguiti: la disponibilità dei dati personali determina in capo a tali soggetti quello che potrebbe definirsi un "potere informatico" capace di far esercitare loro un controllo sociale sugli individui, finanche a giungere ad una totale sopraffazione degli stessi, fenomeno che assumerà sempre più rilievo col passare degli anni[39].

È proprio in ragione di tali mutamenti che muta, di conseguenza, anche "il senso sociale della *privacy,* non più ancorata soltanto al criterio dell'esclusione dell'altro, ma trasformata e rafforzata dal diritto di seguire le proprie informazioni ovunque esse si trovino, e di opporsi alle interferenze"[40].

Proprio in considerazione di tale mutamento, ed alla centralità assunta da questo "nuovo" diritto, ha origine la tutela approntata dal legislatore europeo, il quale, a far data già dagli anni '80 del secolo scorso, ha iniziato a predisporre un sistema di regole che non si innesta su una precedente regolamentazione, ma che enuncia una disciplina del tutto innovativa, com'è nuova la realtà che si intende disciplinare[41].

---

[39] V. G. BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione*, Giuffrè, 1997.

[40] S. RODOTA', *Il mondo nella rete. Quali diritti, quali vincoli,* Laterza, 2014. Sempre Rodotà scrive, in un'altra celebre opera, "*la sequenza quantitativamente più rilevante è quella "persona-informazione-circolazione-controllo", e non più soltanto quella "persona-informazione-segretezza", intorno alla quale è stata costruita la nozione classica di privacy. Il Titolare del diritto alla privacy può esigere forme di "circolazione controllata", piuttosto che interrompere il flusso delle informazioni che lo riguardano*". V. S. RODOTA', *Repertorio di fine secolo*, *op. cit.*, p. 206.

[41] V. CUFFARO, op. cit., p. 11. Aggiunge l'A. "*in effetti, l'esigenza di approntare una regolamentazione dell'attività di trattamento dei dati personali, che è avvertita quasi contestualmente al determinarsi del fenomeno e ne segue costantemente gli sviluppi, nasce su impulso del legislatore comunitario*".

2. La tutela multilivello del diritto alla protezione dei dati personali in Europa

Il sistema di protezione dei dati personali è da sempre stato influenzato dalla forte tensione esistente tra la diversità delle culture costituzionali nazionali e la spinta verso l'unificazione sottesa (pur ricorrendo numerosi elementi di flessibilità) agli ordinamenti sovranazionali[42].

Tale tensione ha dato luogo, nel tempo, allo sviluppo di un articolato sistema di protezione dei dati personali di carattere sovranazionale, sviluppo che ha preso l'avvio sulla base di una tradizione costituzionale comune a ciascun Stato membro. Nei singoli ordinamenti, infatti, è possibile rintracciare un nucleo essenziale di norme finalizzate alla protezione della sfera personale, da interpretarsi non solo come tutela dell'intimità, bensì, ulteriormente, come tutela proiettata verso l'esterno, che passa attraverso la garanzia dei fondamentali requisiti di autonomia e identità individuale. Tale nucleo fondamentale di norme, comune a ciascun ordinamento, è stato oggetto di una "sofisticata"[43] regolamentazione a livello europeo, che ha dato origine alla costruzione del sistema sopracitato, che si caratterizza precipuamente per il fatto di offrire al singolo, con riferimento al trattamento dei suoi dati personali, una tutela "multilivello": accanto alla tutela che deriva direttamente dal proprio ordinamento nazionale, ciascun individuo può infatti godere, ulteriormente, della tutela offerta dalle norme di diretta derivazione europea, nonché dalle eventuali ulteriori norme di carattere sovranazionale, non necessariamente europee.

Con riferimento a queste ultime, in particolare, vengono in rilievo due strumenti adottati da due organismi diversi, *l'Organisation for Economic Cooperation and Development* (OECD) ed il Consiglio d'Europa (CdE). L'OCSE è stato il primo organismo ad affrontare il problema della individuazione dei princìpi cardine della disciplina della protezione dei dati, attraverso l'adozione, nel 1980, delle "*Linee guida sulla protezione della privacy e dei flussi transnazionali dei dati*

[42] Come evidenziato da autorevoli studiosi della materia "*pochi altri diritti appartenenti alla cosiddetta "nuova generazione" possono vantare l'autentica e solida matrice europea che è propria del diritto alla protezione dei dati personali*". V. L. CALIFANO – C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale scientifica, 2019.

[43] A. FABBRICOTTI, L. RAPONI, op. cit., p. 393.

personali"[44], sebbene tali Linee guida costituiscano uno strumento di *soft-law*, e pertanto non possono essere considerate strumenti giuridicamente vincolanti. Al contrario, il CdE ha emanato nel 1981 la *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*, sulla quale si tornerà a breve, che ha costituito il primo e più importante strumento di regolamentazione normativa, di respiro – appunto - internazionale, e non solo europeo.

Come è dato immediatamente evincere, entrambe le discipline citate risalgono agli albori degli anni '80. Tuttavia, è bene sottolineare che il primo vero riconoscimento, e la conseguente prima regolamentazione, del diritto alla "*privacy*", inteso come diritto al corretto trattamento dei propri dati, non è avvenuto nell'ambito delle richiamate organizzazioni sovranazionali, bensì entro gli ordinamenti di alcuni Stati che, già nel corso degli anni Settanta, avevano adottato le relative leggi in materia[45], contestualmente all'avvento delle tecnologie informatiche nelle grandi industrie private e nelle agenzie collaborative, finalizzate alla raccolta, elaborazione e trattamento dei dati personali.

Tali discipline nazionali, tuttavia, presentavano tra loro notevoli divergenze, a causa delle quali veniva ritardato lo sviluppo del processo di integrazione e completamento dell'Unione europea, costituendo le stesse delle vere e proprie

---

[44] *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, annexed to the OECD Council of 23 November 1980*. Tali Linee guida sono state oggetto di una profonda revisione nel 2013, in considerazione dell'evoluzione delle tecnologie, del mercato e dei comportamenti degli utenti

[45] I primi Stati in cui il concetto di *privacy* nella sua accezione "moderna" si inizia a diffondere sono la Svezia e la Germania. Del resto, proprio in Germania si era verificato, già sul finire degli anni '30 uno dei primi casi di trattamento automatizzato dei dati: la distruzione in una sola notte (conosciuta come "notte dei cristalli") di centinaia di vetrine di negozi di ebrei, fu resa possibile grazie all'uso, da parte delle Squadre di Azione Socialista, degli archivi automatizzati IBM del Ministero dell'Interno e dell'Unioncamere tedesca. Tuttavia, occorrerà attendere gli anni '70 per vedere venire alla luce le prime normative in materia di protezione dei dati. Le prime leggi tedesche furono elaborate in Assia e Baviera (approvate rispettivamente il 7 ottobre 1970 e il 12 ottobre 1970), seguirà poi l'emanazione di una legge organica da parte della R.F.T. nel 1977, cui si ispireranno le leggi emanate successivamente in Francia, Norvegia, Danimarca e Austria. In Italia, invece, si arrivò con estremo ritardo alla definizione di una disciplina normativa relativa al diritto alla protezione dei dati personali. Per una accurata e più esauriente ricostruzione storica, si rinvia a G. BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione*, op. cit.; R. PARDOLESI, *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, 32, e F. BIGNAMI, *Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network*, in *Michigan Journal of International Law*, 2005, vol. 26, 818.

barriere immateriali alla libera circolazione delle persone[46]. Tale libertà, infatti, poteva essere resa possibile solo ove associata alla libertà di circolazione dei dati personali degli individui, e, poiché solamente attraverso un'adeguata garanzia della seconda poteva essere tutelata la prima, si era ormai palesata la necessità, proprio in quegli anni, di un intervento da parte del legislatore sovranazionale finalizzato al riavvicinamento delle varie legislazioni, al fine di far venir meno ogni discrasia.

Proprio per tali ragioni, tra gli anni '70 e '80, il Consiglio d'Europa iniziò ad adottare varie risoluzioni, tra le quali spiccano in particolare quelle del 1973[47] e del 1974[48] relative, rispettivamente, alle banche dati private e a quelle pubbliche[49], poiché in esse è possibile rintracciare le linee portanti della già citata Convenzione del 1981.

2.1 La "*Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*" del 28 gennaio 1981, n. 108

La "*Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*"[50], anche conosciuta come Convenzione n. 108, firmata a Strasburgo il 28 gennaio 1981, costituisce l'unico Trattato internazionale esistente in materia di protezione dei dati personali[51], avente come precipuo scopo quello di garantire un livello minimo comune di protezione delle persone fisiche rispetto alle raccolte ed ai trattamenti effettuati

---

[46] F. PIZZETTI, *La tutela della riservatezza nella società contemporanea*, Rubettino, 2010.

[47] *Resolution on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector n. (73) 22*.

[48] *Resolution on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector n. (74) 29*.

[49] In un primo momento, infatti, vengono approfondite principalmente le tematiche connesse alle banche dati elettroniche, lasciando da parte gli altri aspetti della *privacy*.

[50] Consiglio d'Europa, *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*, STCE n. 108, 1981. La Convenzione è stata oggetto, nei recenti anni, di un lungo processo di ammodernamento, anche in considerazione dell'emanazione del Regolamento UE 2016/679, che si è concluso il 18 maggio 2018.

[51] La Convenzione è uno strumento che dimostra "*il germe del diverso approccio di fondo che, nella materia della c.d. informational privacy, tuttora connota l'ordinamento statunitense rispetto a quelli europei (...): impostato su interventi normativi di settore il primo (e, va aggiunto, con una spiccata propensione a favore della self-regulation nel settore privato, nonostante i limiti dalla stessa manifestati); i secondi, invece, caratterizzati da discipline normative a vocazione generalista, integrate dall'operato di autorità di controllo che si vogliono indipendenti e (in modo più marcato nel disegno della Convenzione di Strasburgo) da discipline settoriali*". V. R. LATTANZI, op. cit., p. 14.

mediante elaborazione automatizzata dei dati, nonché rispetto al trasferimento transfrontaliero con Paesi terzi[52].

La Convenzione, ricollegando per la prima volta, in modo espresso, la tutela della protezione dei dati personali alla tutela della riservatezza[53], va ad integrare l'armamentario giuridico europeo, che all'epoca ruotava principalmente intorno all'art. 8 CEDU «*with regard to automatic processing of personal data*» (art. 1, par. 1, Convenzione n. 108/1981)[54].

La Convenzione, inoltre, non limita la propria efficacia ai soli Stati membri dell'Unione, poiché lascia aperta la possibilità, anche agli Stati che non siano membri del Consiglio d'Europa, di ratificarla[55]. Si tratta, in sostanza, di un atto che, seppur elaborato in un contesto regionale, ha una vocazione universale.

Tuttavia, a causa – principalmente - del regime di discrezionalità lasciato alle Parti contraenti, alle quali viene concessa la possibilità sia di ampliare che, eventualmente, di ridurre la tutela del sistema di protezione ivi predisposto[56], è apparso immediatamente evidente come lo strumento in esame non fosse in realtà del tutto idoneo a raggiungere lo scopo di uniformazione prefissato dal legislatore, permettendo anzi scelte normative molto difformi l'una dall'altra, nonostante la condivisione dei princìpi rientranti nel nucleo duro[57].

---

[52] Si segnala, per un'accurata analisi del testo, il commento reso al testo in forma di progetto da parte di Guido Alpa in G. ALPA, *Raccolta di informazioni, protezione dei dati e controllo degli elaboratori elettronici (in margine ad un progetto di convenzione del Consiglio d'Europa)*, in *Foro.it*, 1981, 2, pt. V, c. 27 ss.

[53] L. CALIFANO, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dati personali*, in L. CALIFANO – C. COLAPIETRO, op. cit., p. 4.

[54] V. R. LATTANZI, op. cit., p. 14.

[55] L'art. 23 conferisce al Comitato dei Ministri il potere di invitare ad aderire alla Convenzione gli Stati non membri del Consiglio d'Europa, anche extra-europei.

[56]La Convenzione non è uno strumento *self-executing*, ma vincola gli Stati a conformare il diritto nazionale ai princìpi fondamentali ivi sanciti, e tale conformazione può avvenire attraverso varie misure, che non comprendono solo le leggi costituzionali ed ordinarie o altri atti normativi di grado inferiore, ma altresì i codici deontologici e gli altri istituti di autoregolamentazione. Tuttavia, agli Stati viene offerta anche la possibilità di derogare ai princìpi fondamentali, sebbene tali deroghe debbano essere attuate mediante strumenti di rango legislativo.

[57] Una delle ulteriori carenze della Convenzione n. 108/81 è da rintracciarsi sicuramente nella scelta di limitare l'applicazione delle disposizioni ai soli trattamenti effettuati mediante elaborazione automatica, e non anche quelli manuali. Tale tutela risulta essere del tutto insufficiente, posto che anche gli archivi manuali possono rappresentare un pericolo per la *privacy*, e considerato altresì che la legge in questione può facilmente essere elusa attraverso la creazione di archivi non automatizzati. V. R. PARDOLESI, *Dalla riservatezza*, op. cit., pp. 34-35.

Nonostante ciò, l'emanazione della Convenzione ha indubbiamente rappresentato un momento utile per stimolare, a livello nazionale ed europeo, una "*vera e propria 'cultura della privacy'*"[58]. Cultura che è stata altresì implementata dal lavoro della Corte Europea dei diritti dell'uomo, la quale, a seguito della sua emanazione, ha dato vita ad un'interpretazione evolutiva e funzionale dell'art. 8 CEDU, originariamente concepito per tutelare in via esclusiva la vita privata e familiare, sul portato del concetto di *privacy* intesa in senso tradizionale, ma che nel tempo, in concomitanza con la sempre più pervasiva diffusione delle nuove tecnologie, è diventato l'articolo di riferimento per la tutela, altresì, dei dati personali[59].

L'interpretazione evolutiva dell'art. 8 CEDU si rivelerà molto utile nel decennio successivo, poiché, con l'entrata in vigore del Trattato di Maastricht nel 1992, che all'art. 6 prevede un richiamo espresso alla CEDU ed ai princìpi costituzionali comuni, il "diritto alla tutela della vita privata e familiare", interpretato nella nuova e moderna accezione di "diritto al controllo delle informazioni personali", diventerà un principio generale dell'ordinamento europeo, al quale ogni Stato membro dovrà obbligatoriamente uniformare la propria normativa.

Ma la Convenzione non è stato l'unico strumento mediante il quale il legislatore ha tentato di superare la frammentazione esistente tra le legislazioni nazionali in materia di protezione dei dati. Preso atto del fallimento della Convenzione, infatti, nel 1990 veniva presentata una proposta di direttiva che si poneva come obiettivo quello di garantire la coesistenza di due valori: da un lato, il raggiungimento di un

---

[58] La citazione è tratta da A. FABBRICOTTI, L. RAPONI, *La struttura multilivello della protezione dei dati personali in Europa*, op. cit.. A livello europeo, sono state numerose le raccomandazioni adottate dal Consiglio d'Europa, con la partecipazione attiva degli Stati membri nella redazione delle stesse. Si rinvia nuovamente a G. BUTTARELLI, op. cit., pp. 28-36.

[59] G. RESTA osserva che la giurisprudenza della Corte di Strasburgo «*ha fatto propria una lettura estensiva della formula "vita privata" di cui all'art. 8, affermando in diverse pronunzie l'applicabilità delle relative garanzie anche rispetto all'ipotesi della raccolta e della conservazione dei dati personali*»., V. G. RESTA, *Il diritto alla protezione dei dati personali*, in F. CARDARELLI, S. SICA e V. ZENO-ZENCOVICH, *Il codice dei dati personali. Temi e problemi*, Milano, 2004. In sostanza, con la Convenzione si stabilisce un collegamento speciale tra il diritto alla "*privacy*", sancito dall'art 8 CEDU (anche se, è opportuno ribadirlo per non incorrere in fraintendimenti, dal punto di vista meramente testuale tale disposizione utilizza l'espressione "*private life*") e il diritto alla protezione dei dati (*data protection*) che costituisce un *quid pluris* rispetto al primo. Sulla giurisprudenza della Corte, sia consentito rinviare a O. POLLICINO – M. BASSINI, *sub art. 8*, in R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017, 137 ss.

livello di protezione dei diritti fondamentali della persona, che si prefiggeva essere di grado "elevato", dall'altro, la realizzazione della libera circolazione dei dati personali all'interno della Comunità europea, in quanto funzionale alle esigenze del mercato unico.

2.2 La Direttiva 95/46/CE "relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati"

Gli artt. 100A e 189B del Trattato di Maastricht attribuivano al legislatore europeo la possibilità di adottare, nelle materie di competenza dell'Unione, delle misure di armonizzazione, purché le stesse fossero "finalizzate all'instaurazione del mercato interno".

Sulla scorta di tale previsione, la Commissione CE presentava una proposta di direttiva[60], la cui approvazione – a seguito di numerose modifiche – avveniva nel 1995, ben quindici anni dopo rispetto all'emanazione della Convenzione n. 108/81, e, dunque, in un contesto sociale già profondamente mutato, stante il dilagante sviluppo del World Wide Web[61].

Approvata il 24 ottobre dal Parlamento e dal Consiglio, la Direttiva 95/46/CE "relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati"[62], nel suo preambolo enuncia "l'istituzione e il funzionamento di un mercato interno nel quale, conformemente all'articolo 7 A del Trattato, è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali, esigono non solo che i dati personali possano

[60] La Commissione, in realtà, presentava un "pacchetto" comprendente, tra l'altro: due proposte di direttiva del Consiglio sula protezione dei dati, l'una di tipo orizzontale e l'altra in tema di telecomunicazioni; un progetto di risoluzione dei rappresentanti dei governi riuniti in sede di Consiglio, proteso ad applicare i princìpi della prima proposta ai settori pubblici non disciplinati dal diritto comunitario; una raccomandazione al Consiglio finalizzata all'apertura dei negoziati per l'adesione dell'Unione europea alla Convenzione 108, sulla base di un protocollo aggiuntivo alla Convenzione medesima; una proposta di decisione del Consiglio nel settore della sicurezza dei sistemi d'informazione.

[61] Basti pensare che solo tre anni dopo, nel 1998, vedrà la luce *Google Inc.*, il motore di ricerca oggi più noto e importante al mondo.

[62] Parlamento europeo e Consiglio, Direttiva 95/46/CE del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in GUCE n. L 281 del 23/11/1995.

spostarsi liberamente da uno Stato membro all'altro, ma anche che i diritti fondamentali delle persone fisiche siano del pari tutelati" (considerando n. 3).

Già dalla lettura del preambolo citato è dato evincere chiaramente come la finalità della Direttiva fosse sì quella di offrire agli individui delle garanzie adeguate con riferimento al trattamento dei loro dati, ma ciò al solo fine di favorire maggiormente la circolazione di tali dati tra gli Stati, in quanto, come evidenziato in precedenza, la circolazione dei dati personali è strettamente correlata alla libera circolazione delle persone e dunque alle esigenze del mercato unico.

L'inevitabilità della circolazione dei dati, la necessità di abbattere barriere che possano frapporsi alla stessa, l'importanza di stabilire un livello di tutela equivalente in tutti gli Stati per evitare discriminazioni di trattamento, costituiscono le principali motivazioni che hanno indotto il legislatore a definire una disciplina normativa fondata, come evidenziato da autorevole dottrina, sul binomio "*circolazione e (vs) protezione*" dei dati[63], con ciò volendosi riferire al sistema di contrappesi sul quale è stato fondato l'intero quadro normativo. In ragione di tale bilanciamento, il trattamento può essere posto in essere solo allorquando siano rispettate determinate condizioni, enucleate nell'art. 7 della Direttiva: quando vi sia il consenso della persona interessata, manifestato in maniera inequivocabile (e, con riferimento ai dati sensibili, esplicito); quando il trattamento si riveli necessario per dare esecuzione a un contratto concluso con l'interessato; quando il trattamento serva ad adempiere un obbligo giuridico da parte del titolare del trattamento; quando sia necessario per salvaguardare un interesse essenziale della persona interessata; quando sia necessitato al fine di poter esercitare una funzione di pubblico interesse; quando, infine, sia necessario per perseguire l'interesse legittimo del titolare del trattamento[64].

Al soggetto interessato, vale a dire l'individuo cui i dati si riferiscono, vengono riconosciute una serie di posizioni giuridiche attive: prima fra tutte quella di accesso ai dati che lo riguardano, che prelude altresì ad ulteriori facoltà, quali – ricorrendone i presupposti – la richiesta di rettifica o cancellazione dei dati,

[63] S. SICA, *Verso l'unificazione del diritto europeo alla tutela dei dati personali?*, in S. SICA - V. D'ANTONIO - G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, Cedam, 2016, pp. 1 ss.

[64] Art. 7, Dir. 95/46/CE.

ovvero di opposizione ad un loro ulteriore trattamento, o, ancora, quella volta a conoscere l'origine delle informazioni nonché le categorie dei soggetti cui le stesse sono state comunicate.

Accanto alla previsione di questi diritti, la Direttiva sancisce altresì i princìpi cui il trattamento deve ispirarsi: tra i più importanti si ricordano quello di liceità e correttezza, quello di trasparenza (imperniato sul diritto dell'interessato ad essere informato circa le caratteristiche essenziali del trattamento), quello di pubblicità (che trova la sua massima esplicazione nell'obbligo di tenuta di registri dei trattamenti liberamente consultabili presso le Autorità di controllo), ed ancora quelli di finalità e di sicurezza.

Tuttavia, le garanzie offerte al singolo attraverso, da un lato, il riconoscimento dei diritti di cui sopra, e, dall'altro, l'imposizione dell'obbligo al titolare di conformare il trattamento ai richiamati princìpi, non potevano costituire, da sole, misure sufficienti ad offrire all'interessato una tutela adeguata.

Basti al riguardo considerare come gran parte dei trattamenti si fonda su basi giuridiche diverse da quella del consenso, quali ad esempio quella del legittimo interesse del titolare ovvero quella dell'esercizio di una funzione pubblica: in questi casi l'interessato non può opporre il proprio dissenso al trattamento, avendo solamente l'eventuale possibilità di intervenire in un momento successivo, anche se non è detto che la sua opposizione possa trovare accoglimento in caso di trattamenti obbligatori *ex lege*.

Inoltre, con specifico riferimento ai trattamenti fondati sul consenso, occorre pur sempre considerare che tale "strumento" non ha una valenza negoziale-dispositiva, quanto, piuttosto, meramente "autorizzatoria". È vero infatti che l'interessato, fornendo il proprio consenso, conferisce al titolare la legittimazione a trattare i propri dati personali, continuando a mantenere un controllo sugli stessi[65], tuttavia è vero anche che è il titolare a determinare le finalità, le caratteristiche e le modalità del trattamento, imponendo tali scelte all'interessato, che le subisce, non potendo egli godere di alcun potere di regolamentazione al

[65] D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in Riv. Crit. del Dir. Priv.", 1997, p. 339 ss.

riguardo: ecco perché il consenso assume sempre più le vesti di un mero "assenso al trattamento"[66].

Per tali ragioni, il legislatore ha ritenuto opportuno introdurre, accanto alla tutela imperniata sul controllo individuale da parte dell'interessato (che, come evidenziato, risulta essere piuttosto blanda) una tutela garantita attraverso un controllo di carattere "sociale" sull'operato del titolare, attraverso la previsione dell'obbligo, per ciascun Stato membro, di istituire un organismo nazionale indipendente, che vigili sulla corretta applicazione delle leggi nazionali e dei princìpi fissati dal legislatore comunitario.

Sebbene nell'art. 2 della Direttiva, dedicato alla definizione dei termini utilizzati nella stessa, manchi un riferimento a tale concetto di "autorità di controllo", nel considerando n. 62, la designazione della suddetta (o più) autorità, viene addirittura ritenuta "essenziale"[67], anche alla luce delle indicazioni legislative di carattere internazionale[68].

Proprio sul portato di tali indicazioni, il legislatore ha stabilito, dunque, all'art. 28 l'obbligo per ciascuno Stato di istituire un'Autorità di controllo, autonoma e indipendente, i cui compiti vengono enucleati nell'articolo in questione[69]. La norma lascia poi ai singoli Stati l'onere di disciplinarne la composizione, la

---

[66] D'altronde, sarebbe impensabile per ciascun Titolare negoziare, con il concorso di ogni interessato, le modalità e le caratteristiche di ciascun trattamento: è molto più semplice stabilire finalità e modalità dello stesso che soddisfino le condizioni di liceità previste dalla normativa, e per le quali verrebbe poi prestato un consenso "adesivo" da parte degli interessati. V. F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Le monografie di Contratto e impresa, CEDAM, 2018, in particolare nota n. 19.

[67] Considerando n. 62: "*la designazione di autorità di controllo che agiscano in modo indipendente in ciascuno Stato membro è un elemento essenziale per la tutela delle persone con riguardo al trattamento di dati personali"*.

[68] Oltre alla Convenzione di Strasburgo, si vuol fare riferimento alla Convenzione di applicazione dell'Accordo di *Schengen*, che ha istituito il "*Sistema informativo Schengen*", vale a dire una rete informativa comune per la trasmissione di dati personali con finalità di sicurezza e di ordine pubblico. Tale Convenzione postulava la necessità, per gli Stati aderenti, di dotarsi previamente di una organica disciplina di tutela dei dati personali, nonché di prevedere delle autorità indipendenti con compiti di vigilanza. La Convenzione in questione istituiva inoltre un'Autorità comune di controllo, composta da rappresentanti designati dalle singole autorità nazionali, la cui indipendenza, seppure non prevista esplicitamente dalla Convenzione, può essere desunta da altre circostanze. Un ulteriore atto giuridico a carattere internazionale è la Convenzione di Dublino del 15 giugno 1990 sul diritto d'asilo, che prevede l'istituzione di organismi nazionali preposti al controllo sui flussi transfrontalieri di dati personali. V. R. D'ORAZIO, *Garante per la protezione dei dati personali*, in E. GIANNANTONIO - M.G. LOSANO - V. ZENO-ZENCOVICH (a cura di), *Il trattamento dei dati personali*, Cedam, 1999.

[69] In particolare, la Direttiva specifica che l'indipendenza deve essere piena e deve riguardare non solo le funzioni ispettive e di vigilanza, ma la globalità delle stesse, e dunque l'intero organo.

struttura, nonché le modalità di designazione: è per tale ragione che, nel dare attuazione a tale articolo, gli Stati membri hanno adottato delle discipline normative molto differenti tra loro, almeno dal punto di vista istituzionale: "se, sotto il profilo funzionale, il confronto tra i vari organi nazionali di controllo rivela molti punti di convergenza, per quanto riguarda invece la loro collocazione istituzionale, la loro struttura e composizione, le modalità di nomina e le guarentigie poste a presidio della loro indipendenza il panorama è alquanto disomogeneo"[70].

Ad ogni modo, nonostante le segnalate divergenze, l'introduzione di tali figure istituzionali nell'ambito di ciascun ordinamento, avvalora la tesi secondo la quale il diritto alla protezione dei dati personali inizia a godere, a far data dall'emanazione della Direttiva, di una "proiezione istituzionale"[71], espressione dell'interesse pubblico sotteso all'intera disciplina. L'imposizione di un controllo sociale affidato ad un'autorità indipendente diviene, infatti, la vera chiave di garanzia del sistema di protezione dei dati personali così definito[72]: la tutela approntata non presenta, dunque, carattere preminentemente individualistico, ma coinvolge una specifica responsabilità pubblica[73], indispensabile in un contesto in cui le garanzie tradizionali non sembrano da sole sufficienti a tutelare il singolo individuo, data la capacità dei sistemi informatici e telematici di spiegare effetti che, travalicando il singolo, investono l'intera collettività[74].

---

[70] V. R. D'ORAZIO, il quale mette a confronto, in particolare, l'esperienza francese, in cui è presente la figura della *Commission Nationale de l'informatique et des Libertés* (CNIL); quella inglese, in cui l'organo di tutela rientrerebbe nel novero dei c.d. *quangos*, acronimo di *quasi autonomous non governmental organizations*; e quella tedesca, ove sono presenti più autorità nei diversi ambiti (federale e dei singoli Länder).

[71] La Corte di Giustizia dell'Unione europea, in più occasioni, si è espressa sulle Autorità indipendenti affermando che queste costituiscono «*un elemento essenziale del rispetto della tutela delle persone con riguardo al trattamento dei dati personali*». Cfr. rispettivamente C. Giust. UE, 9-3-2010, C-518/07; C. Giust. UE, 13-5-2014, C-131/12, Google Spain SL, par. 69; C. Giust. UE, 16-10-2012, C-614/10, Commissione europea/Germania, par. 36; C. Giust. UE, 8-4-2014, C-288/12, Commissione europea/Ungheria, par. 47-48; C. Giust. UE, 6-10-2015, C-362/ 14, *Schrems*, par. 40-41.

[72] Le Autorità, utilizzando le parole dell'ex presidente del Garante per la protezione dei dati personali Francesco Pizzetti, costituiscono oggi "la "*longa manus*" dell'Europa, costituendo uno strumento di armonizzazione". V. F. PIZZETTI, *La tutela della riservatezza nella società contemporanea*, op. cit.

[73] S. RODOTA', *Il mondo nella Rete*, op. cit., p. 32.

[74] G. BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione*, op. cit., p. 489.

Accanto alla previsione delle Autorità di controllo, il legislatore europeo aveva altresì previsto l'istituzione di un Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali. Tale Gruppo, anche noto come WP29, sigla derivante dalla traduzione inglese "*Article 29 Working Party*", costituiva l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata, ed era composto da un rappresentante dell'Autorità di controllo di ciascuno Stato membro, da un rappresentante delle istituzioni comunitarie e da un rappresentante della Commissione. Lo stesso è stato oggi sostituito dal Comitato europeo per la protezione dei dati personali, sebbene, tanto la composizione quanto i compiti affidati non siano mutati, ma semplicemente aumentati[75]: i compiti che la precedente Direttiva affidava al WP29 consistevano nell'obbligo di esaminare ogni questione attinente all'applicazione delle norme nazionali di attuazione della normativa, per contribuire alla loro applicazione omogenea; quello di informare la Commissione nel caso di manifeste divergenze di tutela delle persone in materia di trattamento dei dati personali nei diversi Stati membri; quello di redigere pareri sui livelli di tutela in materia di protezione dei dati; ed infine quello di formulare raccomandazioni.

Con l'istituzione del WP29, il legislatore rendeva concreta la cooperazione tra le singole Autorità nazionali, oltre a prevedere un controllo ancora più pregnante del rispetto dell'apparato normativo in materia di protezione dei dati.

2.3 L'attuazione della Direttiva 95/46/CE in Italia

2.3.1 Dalla Legge n. 675 del 31 dicembre 1996…

In Italia, il riconoscimento del diritto alla protezione dei dati personali è avvenuto tardivamente rispetto agli ordinamenti degli altri Paesi europei.

Come si è già avuto modo di osservare, alcuni Stati membri dell'Unione, ancor prima che venisse emanata la Convenzione n. 108/81, si erano dotati di una

[75] Da una lettura del combinato disposto degli artt. 64, 65 e 70 GDPR emerge come, a differenza del WP29, il Comitato abbia non solo compiti di carattere consultivo, da cui deriva il potere di formulare pareri nei casi indicati all'art. 64 GDPR, ma anche poteri decisionali vincolanti che gli derivano dal doversi occupare della composizione delle controversie tra autorità di controllo, ai sensi dell'art. 65 GDPR. Resta, infine, la possibilità per il Comitato di adottare di propria iniziativa una vasta mole di linee guida, raccomandazioni e buone prassi sull'applicazione coerente del GDPR. Cfr. BISTOLFI, BOLOGNINI, PELINO, *Il Regolamento Privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, pp. 655 e ss.

normativa *ad hoc* relativa ai trattamenti dei dati personali. Ciò ha consentito alla giurisprudenza di quegli ordinamenti di elaborare un'indagine approfondita in merito al diritto all'autodeterminazione informativa, indagini che poi sono state d'ausilio al legislatore europeo nella redazione della Direttiva 95/46/CE.

Al contrario, nel nostro ordinamento, si è dovuto attendere l'inizio degli anni '90 per far sì che la discussione sul tema della protezione dei dati personali iniziasse a prendere forma e sostanza, nonostante le ripetute sollecitazioni da parte della dottrina[76], a loro volta determinate dall'evoluzione giurisprudenziale che frattanto si era andata sviluppando, sin dagli anni '50, in merito al diritto alla riservatezza[77], il cui contenuto ricalcava quello del concetto di *privacy* di matrice americana originariamente inteso, vale a dire come diritto a non subire interferenze esterne nella vita privata. Si dovrà attendere, tuttavia, metà degli anni '70 per il primo vero riconoscimento, seppure solo giurisprudenziale, di tale diritto: con la storica sentenza del 1975, la Corte di Cassazione ha infatti riconosciuto il diritto in questione identificandolo quale «tutela di quelle situazioni e vicende strettamente personali e familiari, le quali, anche se verificatesi fuori dal domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, e contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi

[76] Cfr. AULETTA, *Riservatezza e tutela della personalità*, Giuffrè, 1978; G. ALPA - M. BESSONE (a cura di), *Banche dati telematiche e diritti della persona*, Cedam, 1984 in cui possono rintracciarsi diversi contributi in merito.

[77] Cfr. E. ONDEI, *Esiste un diritto alla riservatezza?,* in *Rass. dir. Cinema*, 1955, 66 ss.; C.E. TRAVERSO, *Riservatezza e diritto al rispetto della vita privata*, in Riv. Dir. Industriale, 1963, II, 30 ss. Per quanto riguarda il formante giurisprudenziale, molti casi si sono avuti a partire dagli anni '50, tra cui i più noti sono stati quello riguardante la realizzazione di un film sulla vita privata del tenore Caruso e quello relativo ad una pubblicazione concernente la vicenda di Claretta Petacci. Si trattava di casi in cui giudici di merito e quello di legittimità avevano visioni diametralmente opposte: i primi ritenevano esistente nel nostro ordinamento un diritto alla riservatezza, contrariamente al giudice di legittimità, che sosteneva la mancanza di un dato testuale certo cui poter fare riferimento. Nel primo caso, deciso con sent. n. 4487/1956 (Cass. civ., sez. I, 22 dicembre 1956, n. 4487, in *Giur.it*, 1957, 379) il figlio ed i nipoti del tenore napoletano Caruso intentarono un'azione contro la casa produttrice del film "*Leggenda di una voce*" che narrava, in forma romanzata, episodi ed avvenimenti relativi alla vita del tenore, soprattutto in considerazione di quegli eventi della sua vita che ne mettevano in risalto l'umile estrazione sociale, rispetto ai quali si vantava il diritto alla riservatezza sulla base dell'applicazione analogica della disciplina del diritto all'immagine. Nel secondo caso, deciso con sent. n. 990/1963 (Cass. Civ., sez. I, 20 aprile 1963 n. 990, in *Foro.it*, 1963), i genitori e la sorella di Clara Petacci (amante di Benito Mussolini) chiedevano l'impedimento della pubblicazione di un settimanale in cui veniva narrata la vita privata della donna attraverso l'uso di asserzioni e toni tali da violare la *privacy* della famiglia Petacci (in questo caso si chiedeva la tutela della *privacy* facendo riferimento all'art. 8 CEDU). La Cassazione negò il suddetto diritto, ritenendo piuttosto violato il diritto alla libertà di autodeterminazione della personalità (a causa della divulgazione di notizie che per loro natura erano da ritenersi riservate), fondato sull'art. 2 Cost.

e senza offesa per l'onore, la reputazione o il decoro, non siano giustificate da interessi pubblici preminenti»[78].

Sulla scorta di tali primi approdi giurisprudenziali inerenti il diritto alla riservatezza, hanno poi preso avvio riflessioni ulteriori, volte a valutare la possibilità di ampliare il contenuto di tale diritto, al fine di ricomprendervi ulteriormente la possibilità per l'individuo di esercitare un controllo sulle informazioni che lo riguardano, fuori uscite dalla propria sfera personale, e di esercitare un potere decisionale in merito all'impiego e alla destinazione delle stesse [79]. È proprio in quegli anni che vede luce il lavoro di S. Rodotà, in cui il noto Autore rileva la necessità che la *privacy* non venga più considerata quale accezione di carattere "individualistico" e "negativo", ma piuttosto "collettivo" e "positivo"[80].

Proprio alla luce delle considerazioni di cui sopra, emergeva sempre più la necessità, da un lato, di chiarire le coordinate essenziali del diritto alla riservatezza, e, dall'altro, quella di individuarne un solido fondamento normativo, valutando la possibilità di conglobare in esso la tutela di entrambe le situazioni giuridiche richiamate.

A tal fine, in quegli anni furono presentate varie proposte di legge che, sebbene mai approvate, tuttavia ebbero il pregio di consolidare il contenuto del diritto in questione, mettendone in risalto il nucleo fondamentale[81]. Inoltre, nonostante la mancata approvazione di quelle proposte, si deve dare atto della emanazione di una serie di leggi che *de relato* regolavano alcuni aspetti tipici inerenti lo stesso:

---

[78] Cass. Civ. n. 2129 del 27.5.1975, in Foro.it, 1976, I, 2895. Il caso in esame richiese altresì l'intervento della Corte Costituzionale, la quale, con sentenza del 12.4.1973, n. 38 ha affermato l'esistenza di un diritto alla riservatezza nel nostro ordinamento, ricavabile ai sensi degli artt. 2, 3 c. 2, 13 c. 1 Cost. che tutelano i diritti inviolabili dell'uomo, tra cui è ricompresa la riservatezza, così come l'intimità e la reputazione, che a loro volta sono sanciti espressamente dagli artt. 8 e 10 della CEDU, nonché negli artt. 10 cc., 96 e 97 della L. 22 aprile 1941, n. 633.

[79] Cfr. G. B. FERRI, *Privacy e libertà informatica*, e V. FROSINI, *Diritto alla riservatezza e calcolatori elettronici*, entrambi in G. ALPA – M. BESSONE (a cura di), *Banche dati telematiche e diritti della persona*, Padova, 1984. Il primo Autore rileva come il diritto alla riservatezza si caratterizza, rispettivamente, per l'aspetto negativo che consente alla persona di impedire la raccolta di dati e per l'aspetto positivo che consente "*il potere, cioè del titolare del dato raccolto di conoscere, controllare l'uso, modificare, aggiornare*". Il secondo autore evidenzia invece come il diritto alla riservatezza "*non viene più inteso in senso puramente negativo" ma "in un senso positivo, di affermazione della propria libertà e dignità della persona, di limitazione imposta dall'individuo sul potere informatico*".

[80] S. RODOTA', *La "privacy" tra individuo e collettività*, in *Politica del diritto*, 1974, 5, 545 ss.

[81] Si ricordano i progetti Accade (1981), Picano (1982), Mirabelli (1982), Martinazzoli (1984), Bozzi (1985), Mirabelli-*bis* (1989).

basti pensare alle più note, quali la legge 1° aprile 1981, n. 121, relativa all'amministrazione di pubblica sicurezza e la legge 7 agosto 1990, n. 241 sul procedimento amministrativo, che regolava, tra l'altro, l'accesso ai documenti amministrativi.

Nonostante tali progressi, tuttavia, occorrerà attendere la fine degli anni '90 per la regolamentazione della materia, che avverrà sotto l'impulso della Direttiva 95/46/CE.

Risale, infatti, al 31 dicembre 1996 l'approvazione della Legge n. 675 sulla "*tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*", che permette all'Italia, al contempo, di ratificare la Convenzione n. 108/81[82], di entrare nell'Area Schengen [83] e, soprattutto, di recepire la Direttiva 95/46/CE.

Ed è proprio in concomitanza della approvazione della citata legge, nonché del successivo D. Lgs. n. 196/2003, che verrà dato l'avvio al difficoltoso processo di distinzione del diritto alla riservatezza dal diritto alla protezione dei dati personali[84].

In particolare, nell'art. 1 della menzionata legge è scritto che la stessa mira a garantire «che il trattamento dei dati personali si svolga nel rispetto dei diritti,

---

[82] Si noti l'estremo ritardo con cui l'Italia si è conformata ai parametri internazionali e, contemporaneamente, la celerità con cui invece è stata recepita la Direttiva 95/46/CE (ben prima della scadenza dei tre anni previsti ex art. 32 come termine per conformare gli ordinamenti nazionali): tale celerità si spiega, in ogni caso, proprio in considerazione del grave ritardo nell'adeguamento del diritto interno alla Convenzione n. 108/81. V. C. CASTRONOVO, *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali*, in V. CUFFARO – V. RICCIUTO – Z. ZENO ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, Giuffrè, 1999, p. 189 ss.

[83] L'accordo di Schengen del 1985 relativo alla creazione di uno spazio comune pe la libera circolazione di persone e merci, mediante la progressiva soppressione delle frontiere, richiedeva la preventiva predisposizione di normative e strutture istituzionali (come ad esempio l'Autorità Indipendente) relative alla protezione e al trattamento dei dati personali in collegamento alla tutela degli interessi pubblici relativi al determinarsi di uno "spazio senza frontiere" dove fosse libera la circolazione delle persone e delle merci. Cfr. G. M. SALERNO, *Le origini ed il contesto*, in L. CALIFANO – C. COLAPIETRO, op. cit., p. 65.

[84] È stato rilevato al riguardo che "*la controversia che da tempo si è accesa tra i cultori di questa materia, ben prima che essa approdasse alle rive della nostra legislazione – se la c.d. protezione dei dati costituisca un superamento del diritto alla privacy nei termini di un nuovo diritto della personalità – appare sfuocata. È chiaro infatti, che la riservatezza e l'intimità della sfera giuridica del soggetto costituiscono l'obiettivo terminale pure di questo intervento legislativo. Ma, come sempre, per il giurista il problema è formale, di vera e propria modalità giuridica mediante la quale un dato materiale è divenuto oggetto di tutela. E la modalità giuridica di cui all'art. 1 sembra essere quella di un diritto sui diritti piuttosto che quella di un nuovo diritto della personalità*". V. C. CASTRONOVO, *op. cit.*, p. 193 ss.

delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale»[85].

Nonostante, dunque, l'occasione offerta al legislatore italiano, che in sede di ricezione della Direttiva avrebbe potuto introdurre una previsione normativa specifica al fine di tutelare anche il diritto alla protezione dei dati personali, questi ha preferito piuttosto rimanere ancorato alle tradizionali nozioni di riservatezza e identità personale. Occorrerà attendere la riforma dell'apparato normativo nazionale operata a mezzo del D. Lgs. n. 196/2003 per vedere realizzata la traduzione, in termini di diritto positivo, del diritto alla protezione dei dati personali.

Uno degli aspetti che merita di essere attenzionato con riferimento alla legge in esame è, inoltre, quello relativo all'istituzione del Garante per la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, anche noto in Italia come "Garante per la protezione dei dati personali" o "Garante privacy" (art. 30, 1º co.). Come è stato osservato, è mediante questa legge che "*per via istituzionale" fa (pieno) ingresso nel nostro ordinamento positivo il riferimento alla protezione dei dati personali e, seppure implicitamente, una situazione soggettiva che a quella protezione, garantita da una autorità pubblica, faccia riferimento, sulla scia di quanto previsto dall'art. 28 della Direttiva 95/46/CE*"[86].

Con l'istituzione del Garante privacy viene ampliato il numero delle autorità indipendenti istituite nell'ordinamento italiano sin dai primi anni del secolo scorso[87]. Tuttavia, il Garante privacy, si presenta come un organismo del tutto peculiare, soprattutto in considerazione della stretta connessione intercorrente tra i suoi fini istituzionali e la materia dei diritti fondamentali, aspetto che non è

[85] Stefano Rodotà ha sostenuto che la formulazione dell'articolo in questione è migliore di quella contenuta nella stessa Direttiva 95/46/CE. V. S. RODOTA', *Intervista su Privacy e Libertà*, a cura di Paolo Conti, Editori Laterza, 2005.

[86] S. CALZOLAIO, *op. cit*, p. 613.

[87] Per un approfondimento sulle Autorità Amministrative Indipendenti, si citano, senza pretesa di esaustività, S. CASSESE – C. FRANCHINI (a cura di), *I garanti delle regole*, Bologna 1996, 69 ss.; G. AMATO, *Autorità semi-indipendenti ed autorità di garanzia*, in *Riv. Trim. di diritto pubblico*, 1997; A. PREDIERI, *L'erompere delle Autorità amministrative indipendenti*, Firenze, 1997; L. ARCIDIACONO, *Governo, Autorità indipendenti e pubblica amministrazione*, in S. LABRIOLA (a cura di), *Le autorità indipendenti*, Milano, 1999; F. CARINGELLA, *Le Autorità indipendenti tra neutralità e paragiurisdizionalità*, in *Il Consiglio di Stato*, 2000, 3, 541 ss.; G. P. CIRILLO, *La tutela della privacy nel sistema del nuovo Codice sulla protezione dei dati personali*, CEDAM, 2004, p.129 ss.

rintracciabile nelle *Authorities* fino a quel momento conosciute[88]. La disciplina dell'Autorità, dunque, introduce "degli aspetti innovativi e prima sconosciuti, accentuando l'evoluzione verso funzioni di garanzia rilevanti nella generale dimensione dell'organizzazione sociale e politica"[89].

Per tali ragioni, si è sostenuto che il Garante per la protezione dei dati personali si andasse ad inserire non tanto tra le autorità amministrative, più o meno indipendenti, preposte ad un singolo settore con funzioni di regolazione e di controllo di determinate attività - specie economiche -, quanto piuttosto tra le autorità di garanzia deputate a garantire (anche) l'attuazione di princìpi costituzionali[90].

La previsione dell'Autorità in questione assurge a momento di chiusura (lo stesso Garante viene definito "*istituzione di chiusura*"[91]) del sistema di protezione dei dati.

Attraverso le garanzie di autonomia ed indipendenza - quest'ultima intesa come soggezione alla sola legge - viene infatti garantito che l'attività del Garante sia volta esclusivamente alla tutela del diritto alla protezione dei dati personali, sottraendola a qualsiasi ingerenza o condizionamento da parte del potere politico ed economico, e permettendo così ai singoli di poter beneficiare di un controllo da parte di una istituzione pubblica "neutrale", ossia autonoma rispetto a qualsiasi altro potere statale. Del resto, ciò che differenzia nettamente tutte le Amministrazioni tradizionali dalle Autorità indipendenti è la preminente ed

---

[88] Cfr. G. BUSIA, *Il ruolo dell'Autorità Indipendente per la protezione dei dati personali*, in N. ZORZI GARGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Wolters Kluwer Italia, 2019, p. 293 ss.

[89] R. D'ORAZIO, op. cit., p. 413. L'A., inoltre, prosegue "*l'assunto appare evidente se si collega l'analisi della norma istitutiva della nuova Autorità di garanzia (art. 30, comma 1) alla considerazione dell'ambito materiale riservato alla sua competenza. La circolazione delle informazioni a carattere personale, ove si accolga l'opinione che avverte il superamento della tradizionale prospettiva individualistica del diritto alla privacy, involge profili suscettibili di investire equilibri di portata generale e di incidere sulla stessa distribuzione del potere nella società democratica. In questo quadro, la tutela dei dati (rectius, delle persone, fisiche e giuridiche, rispetto ad utilizzazioni improprie delle informazioni che le riguardano) contribuisce a realizzare le condizioni di trasparenza necessarie al corretto svolgimento di processi decisionali pubblici e privati, i quali fondandosi sulla raccolta e sull'elaborazione di dati possono altrimenti frapporre ostacoli al libero sviluppo della personalità individuale e, sul versante sociale, privilegiare comportamenti uniformi, tali da "rendere più difficile la produzione di nuove identità collettive" e da ridurre di conseguenza "la complessiva capacità di innovazione all'interno del sistema" (Rodotà)*".

[90] G. BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione*, op. cit., p. 494.

[91] R. D'ORAZIO, op. cit., p. 413.

esclusiva preposizione di queste ultime al "settore ordinamentale" di riferimento, rispetto al quale vengono esercitati i poteri attribuiti dalla legge (attività normativa, attività amministrativa in senso stretto, attività di vigilanza e controllo, attività giustiziale)[92], a presidio del neutrale svolgimento dei compiti ad esse affidati.

2.3.2 …al D. Lgs. n. 196 del 30 giugno 2003

Nel 1996, accanto alla legge n. 675/96 fu approvata anche un'articolata legge delega, la. n. 676/96, avente lo scopo di integrare ed adeguare la prima ogni qual volta la sua applicazione pratica lo avesse reso necessario. Si delineava così un tessuto normativo "mobile", poiché attraverso tale legge veniva delegata al Governo l'emanazione (entro diciotto mesi dalla entrata in vigore della disciplina generale sul trattamento dei dati) di "decreti legislativi, recanti disposizioni integrative della legislazione in materie di tutela della persona e di altri soggetti rispetto al trattamento dei dati personali" (art. 1, lett. a), L. 676/96), anche al fine di "garantire la piena attuazione dei principi previsti dalla legislazione in materia di dati personali nell'ambito dei diversi settori di attività nel rispetto dei criteri direttivi e dei principi della normativa comunitaria" (art. 1, lett. b), l. 676/96). Le leggi in questione si presentavano come "atti a struttura normativa complessa"[93]. Dall'8 maggio 1997 al 30 giugno 2003 sono stati emanati nove decreti legislativi e due D.d.p.r., oltre a numerose normative di settore.

Con l'approvazione del D. Lgs. n. 196 del 30 giugno 2003, il legislatore ha messo ordine nel quadro legislativo nazionale esistente, dando così sistematicità all'intera materia[94].

---

[92] G. P. CIRILLO, op cit., p. 148.

[93] V. CUFFARO – V. RICCIUTO (a cura di), *Il trattamento dei dati personali*, *Vol. II, Profili applicativi*, Giappichelli editore, 1999, pp. 16 e ss..

[94] Sono numerosi i commenti alla disciplina del Codice. Solo a titolo esemplificativo, cfr. MONDUCCI-SARTOR, *Il codice in materia di protezione dei dati personali. Commentario sistematico al D. Lgs. 30 giugno 2003 n. 196*, Padova, 2004; ACCIAI, *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice*, Rimini, 2004; F. CARDARELLI – S. SICA – V. ZENO ZENCOVICH (a cura di), *op. cit.*; S. SICA – P. STANZIONE, *La nuova disciplina della privacy. Commento al d.lg. 30 giugno 2003, n. 196*, Bologna, 2004; M. BIANCA – F. BUSNELLI (a cura di*), La protezione dei dati personali*, Padova, 2007, V. CUFFARIO – R. D'ORAZIO – V. RICCIUTO, *Il codice del trattamento dei dati personali*, Torino, 2007.

Si tratta di un testo unico che, pur non contenendo norme regolamentari, è andato oltre la mera ricognizione compilativa delle differenti disposizioni legislative vigenti, armonizzando l'intera normativa, e adeguandola ai princìpi elaborati nel corso degli anni dalla dottrina e dalle letture interpretative offerte dalla giurisprudenza nazionale, oltre che dal Garante per la protezione dei dati personali[95]. Con questo testo, ribattezzato "Codice in materia di protezione dei dati personali", si consolida normativamente la dimensione della tutela dei dati personali[96].

L'art. 1 del codice afferma in particolare che «chiunque ha diritto alla protezione dei dati personali che lo riguardano», mentre l'art. 2 conferma l'autonomia funzionale di tale diritto, ampliando le finalità del codice alla garanzia «che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali».

Dal confronto del primo articolo del Codice con il primo articolo della Legge 675/96 si evince chiaramente il cambio di paradigma che ha interessato il diritto alla protezione dei dati personali, il quale, con il nuovo decreto, viene finalmente positivizzato, manifestando così la volontà del legislatore di costruire un'architettura sistematica e rigorosa, fondata su princìpi specifici, tra cui spicca in particolare quello relativo all'autodeterminazione informativa, che già permeava il modello di protezione dei dati elaborato dalla Direttiva 95/46/CE.

Il diritto alla protezione dei dati personali, infatti, altro non è che un «nuovo diritto all'autodeterminazione informativa, in grado di tutelare i flussi informativi connessi ai dati personali in ogni settore pubblico e privato, estendendo o comunque declinando in termini più ampi il concetto di riservatezza»[97]. Ancora, scrive G. Finocchiaro «il diritto alla protezione dei dati personali consiste nel diritto del soggetto di esercitare un controllo, anche attivo, sui dati che lo riguardano, che si estende dall'accesso alla rettifica. (...) Si afferma espressamente, quindi, nel nostro ordinamento giuridico, l'esistenza di un diritto

[95] G. P. CIRILLO, *op. cit.*, p. 2 ss.
[96] S. CALZOLAIO, op. cit, p. 24.
[97] CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, Napoli, 2016, 15.

alla protezione dei dati personali, distinto da quello alla riservatezza già da tempo riconosciuto nell'ordinamento giuridico italiano. (...) Il diritto alla protezione dei dati personali deve essere considerato distinto dalla libertà negativa di non subire interferenze nella propria vita privata, divenendo la libertà positiva di esercitare un controllo sul flusso delle proprie informazioni. Per questa ragione è frequente il riferimento all'autodeterminazione informativa, intesa come scelta del soggetto di autodefinirsi e determinarsi. Il diritto alla protezione dei dati personali a differenza del diritto all'identità personale, è un diritto al controllo sui dati, non sull'immagine sociale, ed è un controllo in positivo, come declinato dalla disposizione dell'art. 7 del Codice sui diritti dell'interessato, e non in senso negativo»[98].

Presumibilmente, la scelta del legislatore di positivizzare tale diritto, ben otto anni dopo rispetto alla entrata in vigore della Direttiva 95/46/CE, è stata altresì influenzata dalla proclamazione, qualche anno prima, della Carta dei diritti fondamentali dell'Unione Europea, ove, come già evidenziato, viene per la prima volta attribuito, a livello europeo, un rilievo autonomo di carattere "costituzionale" al diritto alla protezione dei dati personali[99], completando così il percorso di affermazione della protezione dei dati personali come autonomo diritto fondamentale[100].

2.4 La "Carta di Nizza" e il Trattato di Lisbona

A circa cinque anni di distanza dalla emanazione della Direttiva 95/46/CE, si ha una svolta importante con riferimento all'inquadramento giuridico del diritto alla protezione dei dati personali in ambito europeo. Come si è avuto modo di anticipare nelle considerazioni introduttive, il nuovo millennio si è aperto con la proclamazione, a Nizza, della Carta dei diritti fondamentali dell'UE (CDFUE), anche conosciuta come "Carta di Nizza".

[98] G. FINOCCHIARO, «*Identità personale (diritto alla)*», in *Digesto Civile*, Agg., Torino, 2010.
[99] Si veda quanto già approfondito nelle Considerazioni introduttive.
[100] V. G. GIANNONE CODIGLIONE, *La tutela della riservatezza*, in S. SICA - V. ZENO ZENCOVICH, *Manuale di diritto dell'informazione e della comunicazione*, Cedam, 2017, p. 292.

La necessità di far venire meno, anche a livello "costituzionale", l'ambivalenza che contraddistingueva ormai da anni il termine *privacy*, trova finalmente, con la proclamazione della Carta, soddisfacimento.

In essa, infatti, come già anticipato, viene attuata la distinzione tra diritto al rispetto della vita privata e familiare, la cui disciplina è rintracciabile nell'art. 7[101], e diritto alla protezione dei dati personali, la cui disciplina è rinvenibile nel distinto art. 8[102]. La nuova norma non si limita, peraltro, a proclamare il diritto in esame, delineandone gli attributi essenziali, ma definisce altresì i princìpi cui deve conformarsi il trattamento nonché alcuni diritti dell'interessato[103]. Inoltre, viene sancito l'obbligo per ciascun Stato di istituire un'Autorità Indipendente avente il compito di sorvegliare il rispetto delle norme in materia di protezione dei dati personali.

La Carta, considerata dai più un testo avente contenuto «ricognitivo, compilativo e codificatorio»[104], finalizzato alla recensione dell'esistente, al fine di semplificarne la conoscenza[105], solo con la successiva emanazione del Trattato di Lisbona acquisterà valore giuridico.

---

[101] Carta di Nizza, art. 7: "*Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni*".

[102] Carta di Nizza, art.8: "*1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 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*."

[103] È stato precisato che «*l'art. 8 della CDFUE – che individua gli elementi essenziali del diritto – dev'esser letto in combinato disposto con l'art. 52, che precisa la «portata dei diritti garantiti», esigendo il rispetto del «contenuto essenziale» dei diritti suddetti nonché la sottoposizione al principio di proporzionalità delle limitazioni apposte alla tutela degli stessi. La Corte di giustizia ha già avuto modo di invalidare in più di un'occasione provvedimenti normativi comunitari giudicati incompatibili con il rango oggi riconosciuto alla protezione dei dati proprio in ragione della violazione del principio di proporzionalità*, così AIELLO, *La protezione dei dati personali dopo il Trattato di Lisbona*, in *Oss. del dir. civ. e comm.*, n. 2/2015, 425-26.

[104] BIFULCO-CARTABIA-CELOTTO, *L'Europa dei diritti*, Bologna, 2001.

[105] Tale lettura interpretativa è stata criticata da S. CALZOLAIO, il quale scrive "*il diritto alla protezione dei dati di carattere personale costituisce un esempio del fatto che così non era e, forse, non poteva essere. In primo luogo, come sin qui si è detto, è certo che il diritto (fondamentale) alla protezione dei dati personali non facesse parte – almeno – della tradizione costituzionale italiana e, a quanto sembra, neanche di un certo numero di altri Stati membri. Si tratta quindi di un diritto (per noi) nuovo. A ben vedere, si può discutere che il "nostro" diritto facesse parte anche dei diritti fondamentali dell'Unione europea: seguendo quanto affermato nelle Spiegazioni allegate alla Carta in riferimento all'art. 8, nessuno dubita della vigenza della dir. 95/46 o del reg. CE 45/2001 (riferito alle istituzioni dell'Unione europea, ex art. 286 TCE) o dell'art. 8 Cedu o della Convenzione del Consiglio d'Europa del 1981. Tuttavia, nessuno di questi atti identifica un diritto fondamentale alla protezione dei dati di carattere personale. Deve*

Il TUE, infatti, all'art. 6, riconosce alla Carta il medesimo valore giuridico dei Trattati (TUE e TFUE) entrati in vigore l'1 dicembre del 2009[106], circostanza questa che determina l'individuazione, nell'art. 8 della Carta, della base giuridica vincolante per la tutela dei dati personali in qualità di diritti fondamentali[107].

Da tale riconoscimento ne deriva una conseguenza di rilievo in punto di riparto di competenze fra Stati membri e Unione, poiché la materia della protezione dei dati personali viene fatta rientrare nel novero delle materie su cui l'Unione esercita la propria sfera di competenza[108].

Con il venir meno della struttura a pilastri, a seguito dell'introduzione del Trattato di Lisbona, e ai sensi dell'articolo 16 del TFUE[109], che riprende pedissequamente

---

pertanto concludersi che, in questo caso – e se si vuole, opportunamente – la Carta ha positivizzato un nuovo diritto fondamentale europeo, fondandosi principalmente sulla giurisprudenza della Corte edu, la quale all'interno del diritto alla vita privata di cui all'art. 8 Cedu riconosce anche la protezione dei dati personali". V. S. CALZOLAIO, *Protezione dei dati personali,* op. cit., p. 618.

[106] Per comodità si riporta il testo dell'art. 6 TUE: «*1. L'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7-12-2000, adattata il 12-12-2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati. Le disposizioni della Carta non estendono in alcun modo le competenze dell'Unione definite nei trattati. I diritti, le libertà e i principi della Carta sono interpretati in conformità delle disposizioni generali del titolo VII della Carta che disciplinano la sua interpretazione e applicazione e tenendo in debito conto le spiegazioni cui si fa riferimento nella Carta, che indicano le fonti di tali disposizioni. 2. L'Unione aderisce alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Tale adesione non modifica le competenze dell'Unione definite nei trattati. 3. I diritti fondamentali, garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e risultanti dalle tradizioni costituzionali comuni agli Stati membri, fanno parte del diritto dell'Unione in quanto principi generali*».

[107] È stata la Corte di Lussemburgo a precisare, ancor prima del Trattato di Lisbona, che la Carta rappresenta il riferimento normativo e assiologico fondamentale nella tutela del diritto alla protezione dei dati personali.

[108] Prima dell'entrata in vigore del trattato di Lisbona, la legislazione in materia di protezione dei dati personali era divisa tra il primo pilastro (protezione dei dati a fini privati e commerciali, soggetta al metodo comunitario) ed il terzo pilastro (protezione dei dati per scopi di ordine pubblico, con decisioni prese a livello intergovernativo). Cfr. B. CORTESE, *La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona*, in *Dir. Un. Eur.*, 2013, n. 2, 313-335; ID., *Art. 16 TFUE*, in TIZZANO (a cura di), *Trattati dell'Unione europea*, A. TIZZANO (a cura di), *Trattati dell'Unione europea*, Giuffrè, Milano, 2013, 445-446; F. BALDUCCI ROMANO, *La protezione dei dati personali nell'Unione europea tra libertà di circolazione e diritti fondamentali dell'uomo*, in *Rivista italiana di diritto pubblico comunitario*, 2015, fasc. 5, 1626; O. LYNSKEY, *The Foundations of EU Data Protection Law*, Oxford, 2015.

[109] L'articolo tecnicamente sostituisce l'art. 286 del Trattato CE e, eccezion fatta per alcune differenze terminologiche, riprende il testo dell'Articolo 151 del "*Trattato che istituisce una Costituzione per l'Europa*" (firmato nel 2004 e mai entrato in vigore). Per comodità se ne riporta il testo: "*1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di*

l'art. 8 della Carta[110], viene infatti previsto che il Parlamento ed il Consiglio stabiliscono le norme relative alla protezione delle persone fisiche in merito al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e delle agenzie dell'Unione, nonché da parte degli Stati membri, nell'esercizio delle attività che rientrano nel campo di applicazione del diritto dell'Unione.

Il nuovo assetto di competenze sancito dal Trattato di Lisbona sarà determinante negli anni successivi, poiché, proprio sulla base dell'art. 16 TFUE - e non più del precedente art. 100 A TCE, verrà varata la riforma del sistema normativo in materia di protezione dei dati personali.

Infatti, mentre in precedenza le basi giuridiche impiegate ai fini della protezione dei dati personali subordinavano l'intervento dell'UE al perseguimento di obiettivi connessi all'attuazione del mercato interno, posponendo così la tutela dell'individuo alla salvaguardia di interessi di carattere economico e politico[111], ora, al contrario, viene conferita all'Unione una competenza concorrente in tema di protezione dei dati personali, a prescindere da una qualsivoglia connessione con la realizzazione di un mercato unico, da ciò derivando una variazione dell'assetto di interessi tutelati, in virtù del quale il diritto alla protezione dei dati personali finalmente viene a prevalere sugli obiettivi economici dell'Unione.

In definitiva, l'articolo 16 del TFUE riconosce per la prima volta la necessità di una disciplina relativa alla protezione dei dati e alla loro libera circolazione che, in modo trasversale, riguardi l'intero diritto dell'Unione[112]. Ed è per tale ragione che la stessa Unione vede evolvere il proprio ruolo, che non si sostanzia più solamente

---

tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti. Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea".

[110] Viene ripresa, altresì, la previsione che sancisce che il rispetto delle norme in materia di protezione dei dati personali sia soggetto al controllo di Autorità indipendenti: ancora una volta, emerge come l'affermazione del diritto alla protezione dei dati personali reca con sé l'esigenza istituzionale di garantire l'esistenza di una tale Autorità. V. S. CALZOLAIO, op. cit., p. 620. Cfr. altresì G. M. SALERNO, il quale evidenzia che la previsione relativa alla presenza, quale garanzia indispensabile e necessaria, delle Autorità indipendenti, acquisisce "*il carattere di principio direttamente conformativo della strutturazione del complessivo sistema europeo – e quindi dei singoli sistemi nazionali – rivolto a disciplinare e regolare la protezione, il trattamento e la circolazione dei dati personali*": in G. M. SALERNO, Le origini e il contesto, op. cit., p. 70.

[111] Prova di ciò è che la Direttiva 95/46/CE, emanata ai sensi del precedente art. 100 A TCE, tutela il trattamento e la conservazione dei dati personali, ma al solo fine di consentirne una maggiore circolazione, fondamentale per la realizzazione del mercato unico europeo.

[112] F. BOEHM, *Information sharing and data protection in the Area of Freedom, Security and Justice*, Springer, Berlin, 2012, p. 116.

nell'onere di vigilare sulla protezione dei dati personali dei cittadini degli Stati membri in tutti gli ambiti, anche quelli tecnologicamente avanzati, ma altresì nel definire e orientare la "politica europea comune dei dati personali"[113].

È sulla scorta di tali importanti novità che il legislatore europeo ha avviato, nel 2012, il lungo dibattito che ha portato poi al varo del cd. "*pacchetto data protection*", contente una serie di disposizioni che aspirano ad una considerazione unitaria e sistemica della materia, che sarà oggetto di approvazione nel 2016. Si tratta del Regolamento UE 2016/679 sulla protezione dei dati e della Direttiva UE 2016/680 sui trattamenti dei dati personali nei settori della prevenzione, del contrasto e della repressione dei crimini[114]. Queste due normative segnano una significativa frattura rispetto al modello precedentemente adottato, anche in considerazione del fatto che ci si trova, nel nuovo millennio, dinanzi a una nuova concezione del dato, che assume una valenza economica di rilievo, come si avrà modo di analizzare nel capitolo successivo. La nuova disciplina, non a caso, viene ridefinita "disciplina del mercato dei dati"[115], il cui carattere saliente è da rintracciare nella sollecitazione agli operatori del trattamento a tenere comportamenti virtuosi, che si sostanziano in obblighi specifici, coerenti con i princìpi di protezione dei dati, in vista del conseguimento di una maggiore affidabilità da parte dei fornitori di dati, cioè, in definitiva, delle stesse persone i cui dati costituiscono oggetto di trattamento, al fine di ottenere una cessione di dati sempre più imponente e, al contempo, "volontaria". Di certo, però, la definizione di "mercato di dati" non deve far dimenticare che la disciplina del trattamento tocca prima di tutto i valori della persona, ed avverte espressamente l'esigenza di tutela delle libertà fondamentali. Semplicemente, si viene a spostare il baricentro della disciplina, mettendo l'accento sulla necessità di limitare preventivamente il rischio insito nel trattamento dei dati personali, attraverso una

[113] V. G. M. SALERNO, Le origini e il contesto, op. cit., p. 71.

[114] Direttiva UE 2016/680 sui trattamenti dei dati personali nei settori della prevenzione, del contrasto e della repressione dei crimini (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio).

[115] V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia: elementi per un bilancio ventennale*, in V. CUFFARO – R. D'ORAZIO – V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli editore, 2019, pp. 3 e ss.

valutazione che, da generale e accentrata presso l'Autorità di controllo, diviene "decentrata" e affidata ai titolari del trattamento[116].

[116] R. TORINO, *La valutazione d'impatto (Data Protection Impact Assessment)*, in V. CUFFARO – R. D'ORAZIO – V. RICCIUTO (a cura di), op. cit., Giappichelli editore, 2019, p. 857.

CAPITOLO SECONDO
IL REGOLAMENTO (UE) 2016/679 E IL "NUOVO" DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI

1. Il retroterra del GDPR: brevi cenni sul cambio di paradigma della nuova disciplina

Il 2016 è stato l'anno che ha segnato una svolta nella evoluzione del diritto alla protezione dei dati personali e della sua tutela. È in tale anno, infatti, che è entrato in vigore il Regolamento Europeo (UE) 2016/679, «relativo alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, e la libera circolazione di tali dati»[117], anche noto come GDPR (*General Data Protection Regulation*)[118], che sostituisce la precedente disciplina delineata nella Direttiva 95/46/CE.

La nuova normativa, testimonianza dei profondi mutamenti che hanno interessato la società contemporanea nell'ultimo decennio, coniuga il principio di protezione dei dati personali con quello relativo alla libera circolazione degli stessi[119], in una sintesi di cui l'informazione costituisce fulcro essenziale.

---

[117] Pubblicato in GUUE del 4 maggio 2016, L 119, pp. 1-88.

[118] Tra i primi commenti alla normativa sia consentito rinviare a S. SICA – V. D'ANTONIO – G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, Cedam, Milano, 2016; BISTOLFI, BOLOGNINI, PELINO, *Il Regolamento Privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*. *Dalla dir. 95/46 al nuovo regolamento europeo*, I, Collana *I diritti nella «rete» della rete*, Giappichelli, Torino, 2016; ID, *Privacy e il diritto europeo alla protezione dei dati personali, Il regolamento europeo 2016/679*, II, Collana *I diritti nella «rete» della rete*, Giappichelli, Torino, 2016; M.G. STANZIONE, *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Eur. dir. priv.,* 2016, p. 1249 ss.; A. SPINA, *Alla ricerca di un modello di regolazione per l'economia dei dati. Commento al regolamento (Ue) 2016/679*, in *Riv. regolaz. merc.*, 2016, p. 143 ss.; G. FINOCCHIARO, *Introduzione al Regolamento europeo sulla protezione dei dati, in «Le Nuove Leggi Civili Commentate»*, 1/2017; G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017.

[119] Tali considerazioni sono di V. Cuffaro, il quale ha aggiunto "*è al riguardo significativo che nel medesimo art. 1 del Regolamento 2016/679 sia poi ribadito, nel comma 2, il diritto alla protezione dei dati personali ed insieme affermato, nel comma 3, che la libera circolazione dei dati personali dell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*". V. V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali*, *Contratto e impresa*, 3/2018, p. 1104-1105. Merita al riguardo una nota anche il considerando n. 4, che recita: «*Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità [...]*» e ulteriormente il considerando n. 6: «*La tecnologia ha trasformato l'economia e le relazioni sociali*

Nuovo elemento catalizzatore dello sviluppo economico e sociale[120], l'informazione si presenta, al contempo, come bene economico e come oggetto di un diritto fondamentale della persona[121]. Tale natura ambivalente riflette il bilanciamento che il legislatore è chiamato ad operare tra due interessi profondamente diversi e tuttavia meritevoli di eguale tutela: la protezione dei diritti e delle libertà fondamentali delle persone fisiche, con particolare riguardo al diritto alla protezione dei dati personali, da un lato, e la libera circolazione dei dati personali, dall'altro, costituendo gli stessi un vero e proprio incentivo alle più innovative attività di impresa[122], e, dunque, un elemento necessario allo sviluppo del mercato.

Ancora una volta, quindi, l'oggetto centrale della regolamentazione è l'informazione, seppure in una veste nuova e diversa rispetto al passato: ad essere tutelata è, infatti, qualunque informazione, di qualsiasi contenuto[123]. Non è un caso che la definizione di "dato personale" contenuta nell'art. 4 del GDPR, come si avrà modo di analizzare, diventa oggetto, nel nuovo impianto normativo, di un notevole ampliamento rispetto alla disciplina precedente. Tale ampliamento, del resto, non è altro che la diretta conseguenza delle modifiche che in questi anni hanno interessato la categoria di "dato personale", e, prima ancora, quella più generale di "dato", di cui il "dato personale" costituisce un'articolazione.

Ma prima di indagare a fondo tale concetto, è necessario passare in rassegna, seppur brevemente, i fenomeni che hanno interessato l'intera società negli ultimi anni, al fine precipuo di comprendere quali nuovi interessi meritevoli di tutela

---

e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione».

[120] A. STAZI – F. CORRADO, *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica*, in *Dir. Inf.*, 2019, p. 443.

[121] G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE 2016/679 e d.lgs. 10 agosto 2018, n. 101*, p. 2.

[122] G. D'IPPOLITO, *Il principio di limitazione delle finalità del trattamento tra data protection e antitrust. Il caso dell'uso secondario di Big Data*, in *Dir. Inf.*, fasc. 6, pp. 943 ss.

[123] V. G. FINOCCHIARO, *Riflessioni sul poliedrico Regolamento europeo sulla privacy*, in *Quaderni costituzionali*, Fasc. 4, dicembre 2018. L'A. precisa "*qualunque informazione, quale che sia il suo contenuto, è oggetto del Regolamento. Il diritto alla protezione dei dati personali deve essere considerato distinto dalla libertà negativa di non subire interferenze nella propria vita privata, al cuore del diritto alla riservatezza, costituendo invece il fondamento della libertà positiva di esercitare un controllo sul flusso delle proprie informazioni*". In un'altra sua opera, l'A. evidenzia come, a rigore, dato e informazione sono termini non coincidenti. V. G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo*, in G. FINOCCHIARO (a cura di), op. cit.

siano venuti in rilievo come diretta conseguenza degli stessi, nonché l'influenza che questi hanno esercitato proprio sulla modifica inerente il concetto di dato personale.

Solo dopo aver compiuto questa operazione preliminare si potrà passare ad una più approfondita indagine relativa al concetto in questione, necessaria in quanto, come in ogni settore giuridico, è solamente attraverso l'analisi e la comprensione dell'oggetto della normativa che è possibile comprendere la *ratio* che ha animato le scelte del legislatore, specialmente quelle più innovative (con particolare riferimento a tutte quelle che ruotano attorno al concetto di rischio e di *accountability*, che verranno attenzionati più avanti).

Alla luce di quanto premesso, l'indagine svolta nel presente capitolo prenderà avvio, come si anticipava, dall'analisi dei fenomeni che hanno interessato la società contemporanea, oggi più che mai digitale e iper-connessa[124]. Tali fenomeni, che si sostanziano nella raccolta sempre più massiccia di informazioni, di qualsiasi genere e tipo, e nel proliferare di sistemi sempre più sofisticati di analisi, che permettono di "ricostruire la vita privata come sommatoria di dati personali"[125], hanno indotto il c.d. processo di datificazione ("*datafication*" o "*datification*")[126], vale a dire il procedimento mediante il quale tutta la realtà viene tradotta in un flusso di informazioni, attraverso il trattamento e l'analisi dei dati in cui la realtà si sostanzia.

Proprio tale processo di datificazione, come si vedrà, ha determinato l'emersione di nuovi e meritevoli interessi di tutela, anche contrapposti tra loro, tutti aventi ad

---

[124] È opinione comune e diffusa che l'avvento e lo sviluppo di tecnologie informatiche sempre più sofisticate abbia apportato delle trasformazioni radicali negli stili di vita quotidiana, nella realtà economica, nelle modalità di esercizio d'impresa, nonché nella percezione di ciascuno di noi, individui di un mondo che, accanto alla dimensione analogica ne conosce una, parallela alla prima, che è quella digitale. Da più parti si tende ad utilizzare l'espressione "*digital disruption*" per indicare questo fenomeno di "digitalizzazione" che permea l'intera società contemporanea. Cfr. AA.VV. (Studio legale Mondini-Rusconi), *Big Data: privacy, gestione, tutele*, *Altalex*, p. 3 ss.

[125] Le parole sono di V. CUFFARO, *op. cit*.

[126] Spesso ci si riferisce alla società contemporanea definendola come "società digitale" o "società datificata". Si è soliti anche riferirsi agli individui che la compongono definendoli "*quantified self*" vale a dire "io quantificato", poiché composto da un insieme di dati. La *datafication*, in particolare *"designa la centralità acquisita dai dati personali in ogni ramo dell'attività umana, suscettibile di essere appunto "dataficata" ovvero ridotta ad informazione e rappresentata mediante serie di dati; e in un'accezione più specifica indica la possibilità, attraverso analisi predittive, di estrarre nuove informazioni a carattere personale da dati già raccolti in precedenza*". V. R. D'ORAZIO, *La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale*, in V. CUFFARO – R. D'ORAZIO – V. RICCIUTO, *op. cit.*, p. 67.

oggetto i dati personali. È per tale ragione che il successivo oggetto di indagine sarà il dato, inteso nella sua nuova accezione.

Infine, si passerà ad analizzare la disciplina normativa predisposta dal legislatore con il nuovo Regolamento 2016/679, soffermandosi sui caratteri più innovativi della stessa, analisi necessaria anche in relazione ai prossimi due capitoli, che si concentreranno nello specifico sulla figura del *Data Protection Officer*.

1.1 Il procedimento di "datafication"…

Con il neologismo "*datafication*" si vuol fare riferimento a quell'insieme di operazioni che, in estrema sintesi, possono suddividersi in registrazione, analisi e riorganizzazione dei dati: attraverso queste operazioni, qualsiasi elemento (fattuale, oggettivo o soggettivo) appartenente alla realtà fenomenica viene convertito in forma quantitativa, al fine specifico di poterlo tabulare, analizzare e riutilizzare a fini applicativi[127]. E poiché "tutto è riconducibile a informazione"[128], è evidente come tale processo si riferisca all'intera realtà fenomenica[129].

Il processo di dataficazione, dunque, si sviluppa, tendenzialmente, su tre fasi. La prima fase è costituita dall'acquisizione (*input*) di tutti i dati che ogni giorno, più o meno consapevolmente, vengono disseminati da persone, istituzioni e società. Tutti noi siamo diventati "*walking data generators*": qualsiasi operazione compiuta attraverso i numerosi strumenti digitali a disposizione (*digital devices*) è infatti in grado, per la strutturazione in connessione, di determinare un flusso di dati che viene acquisito e circola nell'ecosistema digitale, anche a prescindere da una immissione volontaria da parte del titolare dei dati. La possibilità di connessione "*everywhere/everytime*" determina una continua proiezione

[127] V. MAYER SCHONBERGER – K. CUKIER, *Big Data: A Revolution That Will Transform how We Live, Work, and Think*, Boston, 2013, p. 109. Nell'opera viene altresì spiegato che la dataficazione è diversa dalla digitalizzazione, processo, quest'ultimo, mediante il quale si convertono delle informazioni digitali nel codice binario 0-1 in modo che i *computer* li possano processare.

[128] A. MANTELERO, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Le nuove leggi civili commentate*, Cedam, 1/2017, p. 144.

[129] Il processo di dataficazione, avendo ad oggetto l'intera realtà, determina la produzione di un quantitativo di dati enorme: la quantità di dati prodotta nella società contemporanea è calcolabile facendo riferimento alla misura degli *zettabyte*, e precisamente a più di sette *zettabyte*: mille miliardi di miliardi, con riferimento alla sola rete Internet. V ZENO ZENCOVICH, *Il concetto di "autonomia privata" ai tempi dei "Big Data"*, in P. PASSAGLIA – D. POLETTI, *Nodi virtuali, legami informali: Internet alla ricerca di regole*, Pisa University Press, Atti del Convegno Pisa, 7-8 ottobre 2016, p. 32.

dell'individuo sulla Rete, con conseguente proiezione di dati ed informazioni. Sul punto occorre considerare che, accanto ai dati immessi in rete dagli interessati, online oppure offline[130], volontariamente o involontariamente, vi sono poi quelli che vengono direttamente comunicati dalle macchine connesse: basti pensare ai fenomeni dell'*Internet of Things* (IoT) - Internet delle cose[131], o alle *Privacy-Invading Technologies* (PITs) - le tecnologie invasive della *privacy*, che carpiscono i dati in qualsiasi momento, poiché programmati in modo da memorizzare gli stessi automaticamente e senza alcun consenso da parte dell'interessato. Accanto a tali fenomeni di "nuova generazione" occorre considerare, altresì, banalmente, i sistemi e le tecnologie più tradizionali, le quali, essendo spesso meno costose rispetto alle nuove, sono anche quelle più diffuse: basti pensare, a titolo esemplificativo, ai sistemi di videosorveglianza, o a quelli utilizzati per la raccolta di dati di carattere biometrico, i sistemi GPS o RFID 9[132]. Ma non è tutto, poiché non possono essere omessi tutti i casi in cui i dati vengono carpiti attraverso, ad esempio, le violazioni di sistemi informatici[133].

Dunque, la fase di acquisizione (o registrazione), come è facilmente evincibile, si caratterizza per questo accumulo continuativo di dati, i quali possono essere, indistintamente, di carattere non personale o di carattere personale, rientrando peraltro, in quest'ultima tipologia, anche i dati sensibili. Tutti questi dati si

---

[130] La raccolta *offline* può avvenire, ad esempio, attraverso le carte di credito, o i programmi di fedeltà.

[131] L'espressione sarebbe stata utilizzata per la prima volta nel 1999 da Kevin Ashton, direttore di un consorzio di ricerca con sede al Massachussets Institute of Technology (MIT). Il termine viene utilizzato per indicare qualunque oggetto collegato ad Internet, che trasmette informazioni ad un cento di raccolta. Sull'IoT, cfr. A. FINLAY, R. MADIGAN, *GDPR and the Internet of Things: 5 Things You Need to Know*, rinvenibile sul sito web *www.lexology.com*; S. PALANZA, *Internet of things, Big Data e privacy: la triade del futuro*, in *Documenti dell'Istituto Affari Internazionali*, ottobre 2016, rinvenibile sul sito www.iai.it; R. H. WEBER, *Internet of Things – New Security and Privacy Challenges*, in *Computer Law and Security Review*, 2010, p. 23 ss.

[132] Cfr. M. S. ESPOSITO, *Trattamento dei dati personali e rischi correlati, nel prisma dei diritti e delle libertà fondamentali*, in *Dir. Inf.*, fasc. 4, 20189, pp. 1071 ss. L'autrice prosegue nell'elencazione degli esempi di tecnologie volte a carpire un importante quantitativo di dati, facendo riferimento, a titolo esemplificativo, ai sistemi di localizzazione dei veicoli aziendali, impiegati nell'ambito del rapporto di lavoro al fine di rendere maggiormente efficienti determinare attività e/o garantire la sicurezza dei lavoratori, o, ancora, ai braccialetti elettronici ed ai *microchips* sottocutanei, utilizzati sempre nell'ambito del rapporto di lavoro al fine di facilitare o monitorare l'attività dei dipendenti.

[133] Non bisogna pensare a violazioni di sistemi di carattere domestico, ossia alle violazioni di sistemi aziendali che conservano un quantitativo di dati più o meno limitato, poiché relativo ad ambienti geograficamente circoscritti, ma piuttosto a tutte le violazioni che riguardano archivi di dati da dimensioni enormi, come ad esempio i dati di aziende che operano *online* e offrono servizi ad una vasta platea di utenti.

presentano, tuttavia, allo stato grezzo (*raw data*), vale a dire in una consecuzione in forma elettronica di bit da cui non è possibile estrapolare una informazione. Affinché il dato possa esprimere un'informazione, infatti, è necessario che lo stesso venga "lavorato"[134].

Qui viene in rilievo la seconda fase del processo di dataficazione, quella dell'elaborazione (o analisi, o manipolazione) dei dati raccolti: si tratta del procedimento mediante il quale i dati collezionati e processati allo stato grezzo, vengono combinati tra loro e analizzati, producendo così un'informazione, che altro non è che il significato in termini di conoscenza che si può trarre direttamente dal dato processato, o da più dati processati collegati tra loro. Le operazioni di analisi e trattamento vengono svolte da calcolatori (*computers*) e possono basarsi o su logiche computazionali lineari, con algoritmo noto (architetture classiche di *von Neumann*), o su più moderni modelli di A.I.[135], basati su reti neurali e tecniche di autoapprendimento[136].

Una volta avviata l'analisi sulla base di un certo algoritmo, infatti, le macchine, essendo in grado di apprendere dalla loro "esperienza", possono procedere a generare da sé nuovi algoritmi, in grado di raffinare ed ottimizzare l'analisi dei dati [137]. In tal modo, le stesse potranno imprimere, alle masse informative ricavate inizialmente, delle ulteriori logiche di significato. Ciò che si vuole intendere è che

---

[134] BRIGHI, *Il ruolo dei dati informatici nella costruzione della realtà*, Aracne editrice, 2016, 19 ss. e 58 ss.

[135] L'espressione "*Artificial Intelligence*" (A.I., oppure I.A., se ad essere utilizzata è l'espressione italiana "Intelligenza Artificiale") viene utilizzata per descrivere un insieme di programmi e sistemi con funzioni e capacità molto diversi tra loro, che svolgono compiti tradizionalmente svolti dagli esseri umani. In via semplificativa "*l'intelligenza artificiale elabora i dati che riceve, identifica modelli legati a correlazioni ricorrenti, e poi crea e incorpora nuovi modelli; ciò permette al sistema di testare varie ipotesi e trovare nuove soluzioni senza bisogno dell'input di programmazione tradizionale umano*". Cfr. G. COMANDE', *Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità*, in *Analisi Giuridica dell'Economia*, Fascicolo 1, giugno 2019, p. 169.

[136] In alcuni casi vengono utilizzati degli appositi strumenti di intelligenza artificiale come le reti neurali, ossia modelli matematico/informatici di calcolo costituiti da neuroni artificiali che, ad imitazione delle reti neurali biologiche, sono costruiti mediante interconnessioni tra informazioni, e che possono cambiare in maniera adattativa la loro struttura alla luce di dati che scorrono attraverso la rete durante la fase di apprendimento. Cfr. I. N. DA SILVIA, *Artificial Neural Networks – A Practical Course*, Zurich, 2017. L'utilizzo di tali sistemi ed applicazioni A.I. per le attività di trattamento di grandi masse di dati permette (attraverso diverse modalità indicate come *data mining e cleasing*; *data aggregation e integration*; *analysis e modeling*; *data interpretation*) il raggiungimento di risultati che potranno essere previsibili, se basati su criteri e logiche di computo noti, o, al contrario, non previsibili, se basati su criteri e logiche non conosciuti né conoscibili (cd. *hydden layer*, in modalità *machine deep learning,* particolarmente *black box* o *deep learning*).

[137] S. CALZOLAIO, op. cit., p. 598.

le macchine non soltanto elaborano i dati al fine di ricavare le informazioni richieste da chi le programma (vale a dire le informazioni prodotte a seguito delle combinazioni di dati grezzi), ma sono altresì in grado di produrre da sé informazioni nuove e ulteriori, grazie alla loro originale capacità di combinazione, che va oltre la capacità umana di elaborazione e previsione razionale (*data mining*)[138].

Le informazioni così ricavate sono anche note come informazioni "di secondo livello" (cd. informazione da informazione), o *metadati*, ed hanno una importanza strategica nel mercato, poiché le stesse costituiscono vere e proprie fonti di conoscenza delle tendenze del settore analizzato, divenendo, per tale ragione, degli strumenti particolarmente preziosi per le imprese, e non solo[139]. Tale considerazione assume inoltre maggiore significato allorché si consideri che, spesso, le informazioni così ricavate vengono sfruttate non solo da chi produce le macchine che procedono all'analisi, ma anche da altri soggetti, a cui le informazioni possono essere cedute, divenendo in tal modo oggetto di analisi ulteriori e diverse.

La conoscenza così estratta dai *pattern* di dati acquista, dunque, un "nuovo" valore, che viene in rilievo specialmente nella terza fase, che è quella applicativa dei risultati: i dati, infatti, una volta riorganizzati in modo da incrementare non più solo quantitativamente, ma anche qualitativamente, il patrimonio di informazioni disponibili, che assumono così una notevole indole predittiva, vengono utilizzati per prendere delle decisioni che andranno ad impattare sulla collettività: si tratta di decisioni di varia natura, potendo le stesse essere sia politiche che economiche, sia di interessi privati che di interessi pubblici.

---

[138] S. CALZOLAIO, op. cit., p. 599.

[139] L'utilizzo delle metodologie di *data mining* e di applicazioni A.I., permettono di utilizzare le informazioni ricavate nella fase analitica non solo ai fini di un risultato previsibile ed immediato (in termini di *output* di analisi) ma altresì per ricavare, attraverso le modalità di autoapprendimento (ad esempio il cd. *trial and error*), nuove conoscenze e nuove modalità in grado di migliorare *qualitativamente* l'analisi dei dati, giungendo così alla creazione di *data pattern* ulteriori, qualitativamente migliori dei gruppi di informazioni o delle elaborazioni ottenute nella fase analitica, ed in grado di rappresentare non soltanto un valore in termini economici, ma altresì di permettere l'acquisizione di posizioni di vantaggio sul mercato.

1.2 … e il fenomeno "*Big Data*"

Il procedimento di *datafication* sopra descritto ha determinato l'emersione del fenomeno conosciuto anche con l'espressione "*Big Data*"[140]. Tale espressione, sebbene ancora non possa basarsi su una compiuta definizione in termini tecnici o normativi[141], viene comunemente utilizzata per indicare la situazione in cui, attraverso la correlazione di dati differenti tra loro per formato e struttura[142], provenienti da fonti diverse e diversificate, e processati con velocità e attendibilità attraverso modelli tradizionali o applicazioni A.I., è possibile ricavare un patrimonio di informazioni che i singoli *pattern* di dati, se isolatamente considerati, non sarebbero in grado di offrire[143].

Il fenomeno *Big Data* si è imposto sul panorama internazionale sul portato dei più recenti sviluppi della tecnologia e dell'intelligenza artificiale. Le caratteristiche

---

[140] Sul tema, cfr. I. S. RUBINSTEIN, *Big Data: The End of Privacy or a New Beginning?* in *International Data Privacy Law*, 2013, Vol. 3, No. 2; F. DI PORTO (a cura di), *Concorrenza e mercato. Antitrust, Regulation, Consumer Welfare, Intellectual Property - Vol. 23/2016 - Big Data e concorrenza*; F. Pizzetti, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, Giappichelli, 2018, 145 ss.; A. MANTELERO, *Regulating Big Data. The guidelines of the Council of Europe in the context of the European data protection framework*, in *Computer Law and Security Review*, 2017.

[141] "*The concept of extracting knowledge from (large) databases has been researched for years, referred to as data science, data mining, or knowledge discovery from databases. What marked the shift between [last decade and this decade, ndr.] is that the data sets that companies sought to process were too big for the then conventional data processing systems. New technological solutions (…) were needed to work with these quantities of data. Much was expected from these technological developments, and Big Data became a popular term, particularly in the commercial context. And as Big Data became more popular and charged with expectations, its practical applications increased. As a consequence, the term 'Big Data' broadened because it was used shorthand to connote an increasingly diverse array of contexts*". V. M. OOSTVEN, *Identifiability and the applicability of data protection to Big Data*, *International Data Privacy Law*, 2016, Vol. 6, No. 4. Cfr. altresì G. D'ACQUISTO-M. NALDI, *Big Data e privacy by design*, Torino, 2017; G. DELLA MORTE, *Big Data e protezione internazionale dei diritti umani*. *Regole e conflitti*, Napoli, 2018, 178 ss.

[142] G. Giannone Codiglione scrive "*per correlazione si intende il risultato ottenuto dall'analisi e la sovrapposizione di un indefinito numero di informazioni, dal contenuto variabile e non uniforme (…), che disveli l'esistenza di rapporti biunivoci tra uno o più elementi (o valori) tali da potere constatare, sulla base di criteri statistico/percentuali, un certo grado di influenza reciproca*". V. G. GIANNONE CODIGLIONE, *Internet of Things e nuovo Regolamento Privacy*, in S. SICA – V. D'ANTONIO – G.M. RICCIO, op. cit., p. 132.

[143] Una definizione simile è stata accolta dal Parlamento europeo, il quale, nella Risoluzione del Parlamento europeo del 14 marzo 2017 dal titolo "*Le implicazioni dei Big Data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto*", doc. 2016/2225(INI), reperibile online, ha specificato che: "*I Big Data si riferiscono alla raccolta, all'analisi e all'accumulo ricorrente di ingenti quantità di dati, compresi i dati personali, provenienti da una serie di fonti diverse, che sono oggetto di un trattamento automatizzato mediante algoritmi informatici e tecniche avanzate di trattamento dei dati, che usano sia informazioni memorizzate sia in streaming, al fine di individuare determinate correlazioni, tendenze e modelli*".

principali che lo connotano vengono comunemente indicate dalla dottrina americana facendo ricorso alle 5 V[144]:

1. *Volume* (quantità di dati, che è tendenzialmente enorme e costituisce la massima caratterizzazione del fenomeno)
2. *Veracity* (qualità, autenticità e affidabilità dei dati)
3. *Variety* (varietà di fonti da cui i dati vengono estratti e dei formati)
4. *Velocity* (velocità di generazione delle banche dati, nonché alta frequenza nella trasmissione dal punto di origine al punto di raccolta).
5. *Value* (valore/profitto che dipende essenzialmente dal potenziale economico e dalla valenza sociale degli stessi).

Attraverso i sistemi di *Big Data analytics* è possibile risalire, mediante l'elaborazione delle informazioni ricavate nella fase di analisi dell'enorme quantitativo di dati raccolti (personali o meno), sia a gruppi di soggetti che a persone fisiche determinate. A tal fine, a poco rileva che ad essere oggetto di analisi siano pattern di dati personali (rilasciati dall'interessato con il suo consenso, ovvero carpiti senza che questi ne sia a conoscenza) o di dati anonimi, ovvero ancora di dati pseudonimizzati. È possibile infatti che, attraverso la combinazione dei dati raccolti, anche se anonimi o anonimizzati, le macchine riescano comunque a re-identificare i soggetti cui i dati originariamente appartenevano.

La capacità di aggregazione, ormai divenuta sempre più granulare, rilevatrice e invasiva, determina, in sostanza, la possibilità per le macchine di ricostruire profili accurati di milioni di individui, estraendo informazioni anche da frammenti di dati inizialmente non correlati tra loro, ma che vengono combinati in un momento successivo alla raccolta[145].

---

[144] Cfr. G. D'ACQUISTO - M. NALDI, op. cit.; R. BRIGHI, *Il ruolo dei dati informatici nella ricostruzione della realtà,* Aracne editrice, 2017, 41 ss.; M. E. STUCKE – A. P. GRUNES, *Big Data and Competition Policy*, *Oxford University Press*, 2016, p. 16; A. DE MAURO, *A formal definition of Big Data based on its essential features*, *Library Review*, 2016, vol. 65, n. 3, p. 122 ss; VIOLA, *Data mining. Sottrazione, cessione e utilizzo di dati*, in FUMAGALLI MERAVIGLIA (a cura di), *Diritto alla riservatezza e progresso tecnologico*, Napoli, 2015, 189-191; A. GANDOMI – M. HAIDER, *Beyond the hype: Big data concepts, methods and analytics*, in *International Journal of Information Management*, 2015, vol. 35, n. 2.

[145] Un recente studio condotto dall'Università di Stanford ha dato prova di quanto asserito. Alcuni ricercatori dell'Università, infatti, hanno creato una app finalizzata a raccogliere i dati ricavabili dall'utilizzo del dispositivo degli 823 volontari che si sono prestati alla ricerca. Attraverso quest'app sono stati raccolti i metadati di circa 250.000 chiamate e di 1,2 milioni di messaggi di

Ciò che viene in rilievo dall'analisi del fenomeno in questione è che l'obiettivo principale dell'indagine svolta con i *Big Data analytics* non siano tanto gli individui considerati singolarmente, quanto, piuttosto, gruppi di persone, non già preesistenti, bensì creati artificiosamente attraverso l'individuazione di caratteristiche comuni, preferenze e abitudini, individuazione che è resa possibile grazie all'aggregazione dei dati raccolti. Si tratterà, dunque, di gruppi a geometria variabile, plasmati e rimodellati in continuo dagli algoritmi[146], dei quali vengono predetti i futuri comportamenti e rispetto ai quali vengono adottate determinate decisioni, fondate proprio sulle caratteristiche della comunità così individuata[147].

L'impatto economico di questo fenomeno è evidentemente notevole: non a caso si parla ormai di "economia dei dati"[148] e di "*knowledge-based economy*"[149], espressioni che mettono in risalto la necessità, già segnalata dalla dottrina, di "reinventare il capitalismo"[150].

Un report del McKinsey Global Institute (MGI), seppur datato, ha rilevato come, non a caso, i *Big Data* abbiano "un valore significativo nell'economia mondiale, potendo migliorare la produttività e la competizione delle imprese e del settore pubblico e creare un *surplus* economico sostanziale per i consumatori"[151].

Come è dato evincere dal report, dunque, il ricorso ai sistemi di *Big Data analytics* costituisce un considerevole vantaggio competitivo, non solo nel settore

---

testo (frequenza di chiamate e messaggi; durata delle chiamate etc.). Quando questi metadati sono stati incrociati con le informazioni pubbliche dei partecipanti (facilmente reperibili sui vari *social network*) nonché con i registri telefonici disponibili in rete, i ricercatori non solo hanno associato ai dati i nomi delle persone, ma hanno anche individuato informazioni sulla condizione di salute di alcuni di loro, quindi veri e propri dati sensibili. Cfr. MAYER - MUTCHLER- MITCHELL, *Evaluating the privacy properties of telephone metadata*, in *Proceedings of the National Academy of Sciences*, n. 20/2016, 5536 ss., rinvenibile al link *https://pdfs.semanticscholar.org/dbe1/07ce415a8252009f764afa0a058693596c64.pdf?_ga=2.75105106.1789856331.1576169011-2066176090.1576169011*.

[146] A. MANTELERO, op. cit.

[147] M.S ESPOSITO, op. cit.

[148] V. BAGNOLI, *The Big Data relevant market*, in *Concorrenza e mercato*, fasc. 1, p. 79 ss.

[149] G. PITRUZZELLA, *Big Data, Competition and Privacy: a look from the antitrust perspective*, in *Concorrenza e Mercato*, fasc. 1, 2016, p. 16. L'espressione richiama la nota formula usata da S. Rodotà, che si riferiva alla società contemporanea definendola "società della conoscenza". V. S. RODOTA', *Il diritto di avere diritti*, Bari, 2013, p. 135.

[150] V. MAYER SCHONBERGER – T. RAMGE, *Reinventare il capitalismo nell'era dei Big Data*, trad. di G. Maugeri, Egea, 2018, p. 81 ss. Cfr. altresì ITMedia Consulting Bocconi, *L'economia dei dati. Tendenze di mercato e prospettive di policy*, Roma, Gennaio 2018, reperibile al seguente link: *www.itmedia-consulting.com/it/highlights/1187-leconomia-dei-dati-tendenze-di-mercato-e-prospettive-di-policy-lostudiofondamentale-sui-big-data-2.html*, p. 16.

[151] McKinsey Global Institute, *'Big Data: The Next Frontier for Innovation, Competition, and Productivity'*, 1 (May 2011).

privato, ma anche in ambito pubblicistico. Se, difatti, appare di immediata comprensione come l'impresa (specie quella operante *online*, per la quale i dati costituiscono l'oggetto principale della propria attività imprenditoriale[152], nonché il suo principale fattore di sviluppo[153]) possa giovarsi delle tecniche impiegate e dei risultati ottenuti per migliorare la propria presenza sul mercato e posizionare i propri prodotti e servizi[154], è necessario comprendere come anche i soggetti pubblici possono sfruttare tali sistemi per molteplici finalità, alcune delle quali di indubbio vantaggio per i cittadini[155] (peraltro, non soltanto quelli europei, ma anche quelli appartenenti ad altri Stati membri[156]).

---

[152] G. Giannone Codiglione evidenzia che "*negli ultimi anni, il regime di utilizzo dei dati da parte dei prestatori ha superato la mera funzione di volano delle strategie commerciali (si pensi alle preferenze d'acquisto desumibili dal c.d. profiling e alle proposte individuali effettuabili attraverso il behavioural advertising): sono i dati stessi l'oggetto principale dell'attività imprenditoriale. Il dato – sia esso personale che anonimo – viene captato, veicolato, trattato e nella maggior parte conservato ed accumulato, rappresentando una forma di "capitale" diverso e alternativo al plusvalore ottenuto dalla vendita dei servizi o degli spazi pubblicitari*" v. G. GIANNONE CODIGLIONE, *Libertà d'impresa, concorrenza e neutralità della Rete nel mercato transnazionale dei dati personali*, in *Dir. Inf.*, 2015, 4-5, p. 909 ss. (l'articolo può essere altresì rintracciato al seguente link *http://romatrepress.uniroma3.it/ojs/index.php/PTD/article/view/11/11*).Cfr., altresì, DI PORTO, *Big Data e concorrenza*, CeM, n. spec. 23/2016, 5 ss.

[153] Deve altresì evidenziarsi come le principali aziende operanti *online*, quali Google, Facebook, Twitter, hanno fatto dei dati il loro modello di business: si legge in A. ESTEVE, *The business of personal data: Google, Facebook, and privacy issues in the EU and the USA*, *International Data Privacy Law*, 2017, Vol. 7, No. 1: "*personal data has become a new source of economic value. Once processed and classified they provide relevant information for companies about people's interests and activities, which is extremely useful for advertising. Some of the largest Internet companies, such as Google, Facebook, and Twitter, are built on the economics of personal data. Their activities in this area show the importance of collecting, aggregating, analysing, and monetizing personal data*".

[154] È stato acutamente osservato che "*da un'ottica economica, i BD (Big Data, ndr) rappresentano il nuovo asset delle imprese operanti in rete, un'essential facility secondo l'accezione della Corte di giustizia, non diversamente da quanto lo sia stata la rete fissa per le Telco, fermo restando le diversità tra i due termini. La rete è il risultato d'investimenti, cioè esiste grazie all'impiego di energie economiche del suo dominus; queste masse di dati invece sono create dai cittadini della rete, che con noncuranza lasciano pezzi di sé durante la navigazione. Sta accadendo in Internet quanto capitava a Pollicino, che nell'attraversare il bosco lasciava cadere a terra briciole di pane per ritrovare la via di casa. Anche noi durante la navigazione lasciamo cadere frammenti della nostra identità, che raccolti e riorganizzati da chi verrà dopo comporranno il patrimonio virtuale della sua attività d'impresa, cioè gioveranno fondamentalmente a chi li ha raccolti, non alla persona alla quale i dati appartenevano*", V. G. DE MINICO, *Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria*, in *Dir. Pubb.*, fasc. 1, gennaio-aprile 2019, p. 90.

[155] Il valore delle informazioni è tanto più importante allorquando si consideri la possibilità che le stesse possano essere utilizzate da ricercatori, politici, imprenditori a supporto della ricerca scientifica, delle scelte politiche, dell'innovazione. V. M. ALTMAN, A. WOOD, D. R. O'BRIEN, U. GASSER, *Practical approaches to Big Data privacy over time, International Data Privacy Law*, 2018, Vol. 8, N. 1, p. 29 ss. La dottrina, a tal riguardo, ha distinto tre modelli esplicativi delle potenzialità dei *Big Data* nel settore pubblico, potenzialità che si ripercuotono favorevolmente sulla collettività. Il primo è dato dalla possibilità, attraverso la capacità di segmentazione della

Tuttavia, nonostante i considerevoli vantaggi[157], tanto per coloro che vengono in possesso delle informazioni – siano essi pubblici o privati - quanto per i soggetti che vengono "profilati", ben potrebbero esserci degli effetti distorsivi e negativi proprio nei confronti di questi ultimi: le informazioni, infatti, potrebbero essere utilizzate da coloro che le detengono con finalità discriminatorie o invasive, ad esempio al fine di prendere decisioni che possono incidere negativamente sulla vita di ciascun individuo (si pensi, ad esempio, al *rating* del credito, ai rapporti di

---

popolazione in gruppi di persone accomunate da caratteristiche omogenee in un determinato ambito, di attuare interventi mirati in quell'ambito; il secondo è correlato alla capacità di individuare, attraverso la promozione dei princìpi di trasparenza e partecipazione, le esigenze di tali gruppi di persone al fine di migliorare le prestazioni in loro favore; il terzo è dato dalla possibilità di sostituire certe decisioni umane con algoritmi automatizzati, con importanti vantaggi per il settore pubblico in termini di efficienza. V. G. M. RUOTOLO, *I dati non personali: l'emersione dei Big Data nel diritto dell'Unione europea*, in *Studi sull'integrazione europea*, 1/2018, p. 105.

[156] La possibilità di esercitare un controllo pubblico anche su dati riferibili a cittadini extraeuropei determina un fenomeno di *disclousure* globale della vita istituzionale ed amministrativa di qualsiasi Stato e delle persone ivi residenti: tale controllo esterno rievoca in qualche modo il tema della sovranità e della relazione esclusiva di cittadinanza tra persona e Stato di appartenenza, poiché viene data la possibilità allo Stato di accedere a dati di cittadini appartenenti ad un altro Stato, anche non membro dell'Unione. V. S. CALZOLAIO, op. cit. p. 601. Le riflessioni della dottrina, tanto statunitense quanto europea, in merito alla relazione tra controllo sui dati e sovranità dello Stato sono numerose. Sebbene vi sia chi abbia sostenuto che i dati non possono considerarsi connessi ad alcuno specifico territorio; e sono slegati dal concetto di cittadinanza (v. J. DASKAL, *The Un-Territoriality of Data*, in Yale L.J, 2016), in verità, com'è noto, questa affermazione non può trovare conforto nella normativa europea, anche soltanto in virtù della considerazione per cui la protezione dei dati personali è riconosciuta come diritto fondamentale dall'art. 8 della Carta Europea dei Diritti Fondamentali, e dunque si tratta di una situazione giuridica strettamente legata alla cittadinanza europea. Per una ricostruzione analitica delle molteplici questioni legate al concetto di sovranità, si rinvia anche a G. RESTA – V. ZENO ZENCOVICH, *La protezione transnazionale dei dati personali, Dai "safe harbour principles" al "Privacy Shield"*, *Roma TrE-Press*, 2016: l'opera, infatti, attraverso l'analisi della nota sentenza resa dalla Corte di Giustizia nel caso *Schrems*, pone l'accento sui problemi che il trasferimento transfrontaliero dei dati personali determina in merito all'individuazione delle norme di diritto da applicare ai trattamenti transfrontalieri, e si occupa del concetto di sovranità statale, anche facendo riferimento al fenomeno dei *Big Data*. Si veda, altresì, per i problemi inerenti i controlli esercitati ai fini di polizia predittiva e sicurezza nazionale, il contributo di A. BONFANTI*, L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta La giurisprudenza della Corte di giustizia in materia di digital privacy come osservatorio privilegiato*, in *Medialaws*, fasc. 3/2018, p. 206 ss.

[157] Quando si fa riferimento alla realtà dei *Big Data* ed in particolare ai benefici che dalla stessa possano derivarne, si tende spesso a richiamare il concetto di "*Data Driven Innovation*", che fa riferimento alla capacità, tanto delle imprese quanto degli organismi pubblici, di utilizzare le informazioni derivanti dalle analisi dei dati al fine di prendere decisioni consapevoli o di sviluppare prodotti e servizi migliori, in grado di semplificare la vita quotidiana degli individui e delle organizzazioni, in modo che l'attività di analisi dei dati possa essere un fattore chiave per lo sviluppo economico e sociale. Inoltre, come stimato dall'OCSE, alla *Data Driven Innovation* è correlata una crescita della produttività delle imprese del 5-10%, ed una riduzione dei costi amministrati per gli enti pubblici del 15-20% grazie a una maggiore efficienza, un maggiore gettito fiscale ed un minore rischio di frodi o errori. V. A. STAZI – F. CORRADO, op. cit., pp. 448-451.

lavoro[158] o alla possibilità di ottenere una copertura assicurativa[159]) o addirittura al fine di condizionamento dell'opinione pubblica[160].

[158] Si pensi, a mero titolo esemplificativo, ad un'azienda che determina la propria politica assunzionale sulla base di criteri che derivano direttamente dalle elaborazioni di *Big Data*. Oppure, all'utilizzo di sistemi di rilevazione della posizione dei veicoli attraverso tecnologia GPS con finalità di *fleet management*, cioè controllo della flotta aziendale. Come già evidenziato da attenta dottrina "*attraverso i rilevatori montati sui veicoli, ma anche sulle dotazioni informatiche in uso ai dipendenti, è possibile svolgere diverse operazioni di monitoraggio, sia in relazione agli spostamenti che allo stato dei veicoli, nonché al funzionamento degli stessi (si pensi, ad esempi, ai sensori relativi alla distribuzione del carburante o al funzionamento dei container che devono mantenere determinati livelli di temperatura). Le attività di monitoraggio e quelle, conseguenti, di trattamento dei dati raccolti non determinano problemi quando siano effettuate senza possibilità di riferimento dei dati ai singoli lavoratori, ma, viceversa, devono essere valutati alla luce della normativa a tutela della privacy in tutte le ipotesi nelle quali il datore di lavoro sia in grado, attraverso l'incrocio dei dati, di esercitare un controllo sul lavoratore affidatario del veicolo o del dispositivo mobile. Tale ordine di preoccupazione risulta all'attenzione, a livello europeo dal Gruppo di Lavoro Articolo29: si considerino, sul punto, alcune precisazioni in ordine alla diffusione ed alla funzione dei sistemi ("con il rapido sviluppo tecnologico e l'ampia diffusione di dispositivi mobili intelligenti, si sta sviluppando un'intera nuova categoria di servizi basati sulla geolocalizzaizone (...) la tecnologia dei dispositivi mobili intelligenti consente il monitoraggio costante dei dati di localizzazione" - GL29, parere 13/2011 adottato il 16.5.2011- WP185) ed al pericolo che essi possano sottendere attività di trattamento di dati personali ("il trattamento di dati che consente al datore di lavoro di raccogliere dati relativi alla localizzazione di un dipendente, sia direttamente che indirettamente, attraverso la localizzazione del veicolo utilizzato o di un componente di esso, comporta il trattamento di dati personali ed è soggetto alle norme della direttiva 95/46/CE - GL parere del 25.11.2005 - WP115)*". Accanto alle ipotesi summenzionate, preme in ogni caso sottolineare come i rapporti di lavoro costituiscono oggi uno dei terreni d'elezione delle conseguenze della pervasività del fenomeno tecnologico. L'A. rileva, a tal riguardo, che "*proprio l'incremento, qualitativo e quantitativo, delle dotazioni tecnologiche e delle risorse telematiche, peraltro, ha ampliato le possibilità di ingerenza e controllo da parte del datore di lavoro sui dati e le informazioni che riguardano il lavoratore, e non solo con riferimento ai dati da questi comunicati (per i quali, è stato rilasciato apposito consenso) o relativi allo svolgimento della prestazione di lavoro e degli obblighi ad essa inerenti (quindi riferibili ad un interesse diretto del datore), ma altresì a tutta una serie di dati ed informazioni che afferiscono alla più riservata sfera della "privacy" del lavoratore ma che, ugualmente, risultano esposte a rischi di ingerenza (illecita)*" . V. A. BUSACCA, *88. Trattamento dei dati nell'ambito dei rapporti di lavoro*, in G.M. RICCIO - G. SCORZA – E. BELISARIO, *GDPR e Normativa Privacy Commentario*, Wolters Kluver, Milano, 2018.

[159] Vi è stato più di un caso in cui le compagnie assicurative si siano rifiutate di stipulare una polizza sulla base dei dati ottenuti da vari *database* contenenti i valori della pressione sanguigna e della frequenza cardiaca misurati in modo continuo e automatico con uno *smartwatch*.

[160] Si pensi, ad esempio, all'incidenza su scelte individuali di rilevanza pubblica: ciò può avvenire ad esempio attraverso l'applicazione della *nudges theory*, una forma di architettura delle informazioni che mira ad alterare il comportamento delle persone in modo prevedibile, senza però proibire certe opzioni o offrire particolari incentivi. V. GM. RUOTOLO, op. cit., p. 107 ove si legge "*Nelle sue prime modalità di applicazione questa tecnica ha assunto forme soft, in quanto statiche (c.d. static nudges, appunto, come nel caso della collocazione di merci in un certo ordine per invogliare l'acquisto di una sola di esse), ma nudges dinamici, modificati in tempo reale sulla scorta dell'elaborazione di Big Data, possono oggi essere estremamente potenti e pervasivi*". O, ancora, si pensi al noto caso di "*Cambridge Analytica*", e all'ipotizzato utilizzo dei dati per orientare il libero esercizio del voto dei cittadini. Alexander Nix, amministratore delegato della *Cambridge Analytica* e consulente di Donald Trump in occasione delle elezioni presidenziali del 2016, in un'intervista pubblicata su La Stampa l'8 settembre 2016 sotto il titolo "*Nix, il cervello della campagna elettorale di Trump: "Grazie ai Big Data sappiamo cosa vogliono i cittadini"* ha dichiarato che: «*nel 2008 abbiamo visto come la campagna dei Democratici abbia fatto ampio*

La pervasività del fenomeno passato in rassegna fa evincere chiaramente come, accanto all'interesse dei singoli, venga a sorgere un ulteriore interesse, di natura collettiva, avente ad oggetto il diritto ad un corretto uso delle informazioni raccolte.

Tuttavia, occorre pur sempre considerare che oggetto di tutela non debba essere considerato solo l'interesse dei soggetti "passivi", poiché a venire in rilievo è anche quello di coloro, soggetti pubblici o privati, che dal fenomeno traggono vantaggi piuttosto rilevanti, soprattutto di carattere economico.

L'emersione di un interesse di carattere collettivo, che va a sommarsi a quello individuale, nonché la necessità di un bilanciamento fra i contrapposti interessi degli attori coinvolti, ha determinato la necessità di una revisione dell'apparato normativo di tutela, che il legislatore europeo ha tentato di mettere in atto attraverso l'emanazione del Regolamento 2016/679. Tale normativa, infatti, pur riferendosi, nello specifico, alla tutela dei dati personali, non sembra considerare più, come anticipato, il concetto di dato personale tradizionalmente inteso, stante tutte le conseguenze che si sono riverberate sullo stesso. Prima di procedere all'analisi della nuova normativa, pertanto, si ritiene indispensabile soffermarsi sul mutamento che ha interessato il dato e la sua natura.

2. Le ricadute del fenomeno "*Big Data*" sulla natura del "dato personale"

L'analisi condotta nel precedente paragrafo ha messo in rilievo quella che risulta essere la principale caratterizzazione della società contemporanea, vale a dire l'essere la stessa oggetto di un continuo procedimento di dataficazione, in virtù del quale le macchine, che rappresentano i principali attori nello scenario ivi descritto, analizzano e combinano tra loro dati raccolti dalle fonti più disparate, al fine di estrarre da questi delle informazioni, anche qualitativamente rilevanti, che hanno un valore economico piuttosto significativo, e che consentono a coloro che li posseggono di condizionare la collettività e, conseguentemente, ogni singolo individuo.

---

uso dei dati digitali per identificare e persuadere gli elettori, soprattutto con i social media. Questo è stato un fattore centrale nel cambiamento degli equilibri anche perché i Repubblicani erano rimasti indietro nell'uso delle tecnologie, mentre in passato erano stati all'avanguardia. Ora si è verificato un nuovo sorpasso in questo campo da parte repubblicana, con grandi investimenti e la mobilitazione di ingenti risorse».

Tale fenomeno determina, come già evidenziato, delle ricadute importanti con riferimento al concetto di dato, ed in particolare quello di dato personale.

Anzitutto, occorre considerare che, nei trattamenti effettuati dalle macchine, i dati personali che vengono in rilievo non sono soltanto quelli che costituiscono, tra gli altri, gli *inputs* del sistema, potendo esser definiti tali anche gli *outputs*, vale a dire i dati (o meglio, le informazioni) prodotti dalle macchine, siano essi intermedi e/o conclusivi. Le macchine, infatti, attraverso la combinazione dei dati allo stato grezzo a loro disposizione, sono in grado di risalire anche a individui specifici, e dunque a dei dati personali. Tali dati (anche denominati "dati inferiti"), derivati in via computazionale (vale a dire generati dagli algoritmi del sistema automatizzato in virtù di processi di derivazione), presentano certamente un carattere innovativo rispetto al passato, avendo una propria peculiare identità nella categoria di "dati personali" tradizionalmente intesa, in quanto gli stessi non sono riconducibili né a quelli «raccolti presso l'interessato», né a quelli «osservati sull'interessato», né a quelli comunicati da altri e diversi titolari del trattamento.

Stante, dunque, la capacità delle macchine di ricavare dati personali dall'analisi di dati anche anonimi o anonimizzati, si evince chiaramente come, tendenzialmente, nessun dato possa, allo stato attuale, considerarsi realmente anonimo[161], poiché, se combinato con altri, può determinare l'acquisizione di un dato personale, e dunque rendere identificabile, potenzialmente, qualsiasi soggetto.

Per tale ragione, ci si è chiesti se la normativa in materia di protezione dei dati personali debba essere o meno estesa sino al punto da ricomprendere, nel suo raggio d'azione, non soltanto i dati personali tradizionalmente intesi, ma altresì i dati non personali, per la loro potenzialità intrinseca di "produrre" dati personali.

La nozione di "dato personale", così, vedrebbe mutare la propria natura, che già nei precedenti anni era stata messa notevolmente sotto pressione dalla evoluzione tecnologica.

Volendosi per un momento attenere al dato testuale, occorre considerare che ai sensi dell'art. 4 del GDPR, per "dato personale" si intende "qualsiasi

[161] La definizione di "dato anonimo" si può ricavare dal considerando n. 26 del GDPR, che riferendosi ad essi li definiscequali "*informazioni che non si riferiscono a una persona fisica identificata o identificabile*". Cfr., sul tema, S. BOURDILLON-KNIGHT, *Anonymous data v. personal data-a false debate: an EU perspective on anonymization, pseudonymization and personal data*", in *Wisconsin International Law Journal*, n. 2/2016, 284 ss.

informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale"[162]. Si tratta di una nozione assai ampia, in cui risalta con ogni evidenza l'estensione degli esempi di informazioni che allo stato attuale identificano o rendono identificabile una persona.

Ed è proprio sulla base del concetto di "identificabilità", che presenta un elevato coefficiente di astrazione e flessibilità[163], che si giocherebbe la possibilità di estendere l'applicabilità del GDPR anche ai dati di carattere non personale: partendo, infatti, dall'assunto per cui, attraverso la combinazione di più dati anonimi o anonimizzati, è possibile giungere alla ricostruzione di un profilo individuale più o meno dettagliato di qualsiasi persona, e dunque di venire a conoscenza di dati personali che ricadrebbero poi nella regolamentazione del GDPR, si è ritenuto che la possibilità di estendere l'applicabilità della normativa già alla fase iniziale del trattamento (quello della raccolta), qualificando come "personali" anche dati che in realtà non lo sono, potrebbe essere utile al fine di garantire una maggiore tutela della collettività. Tale possibilità troverebbe la propria *ratio* anche nella disposizione di cui al considerando n. 26 GDPR, con

---

[162] Come ha avuto modo di evidenziare S. Sica, "*appare ribadita, ed anzi rafforzata, comunque, la scelta di una nozione di dato personale persino al limite della "genericità", ma in realtà, con funzione di onnicomprensività, per un verso, e di capacità di attrazione di nuove situazioni non previste né prevedibili ex ante dal legislatore*". V. S. SICA, *Verso l'unificazione del diritto europeo alla tutela dei dati personali?,* in S. SICA – V. D'ANTONIO – G.M. RICCIO, op. cit., p. 5. Cfr. altresì C. OGRISEG, la quale evidenzia che l'ampia definizione utilizzata dal legislatore recepisce i risultati delle riflessioni del WP29 ed altresì rileva come l'impressione che si ricava è quella di un "*ampio aggiornamento della nozione di dato personale*". V. C. OGRISEG, *Il Regolamento UE n. 2016/679 e la protezione dei dati nelle dinamiche giuslavoristiche: la tutela riservata al dipendente*, in *Labour & Law Issues*, 2016, n. 2. Per un'analisi della nozione di dato personale nella Direttiva 95/46/CE e nel Codice privacy italiano, sia consentito rinviare a M. ATELLI – M. MAZZEO, *Le definizioni del Codice dei dati personali*, in V. CUFFARO – R. D'ORAZIO – V. RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, Torino, 2007, 33 ss.; F. MODAFFERI, *Lezioni di diritto alla protezione dei dati personali, alla riservatezza e all'identità personale*, Roma, 2015, 115; G. P. CIRILLO, *Codice sulla protezione dei dati personali*, Milano, 2004, 66 ss.

[163] Le parole sono di E. PELINO, *Identificazione, identificabilità, identificativo*, in BISTOLFI, BOLOGNINI, PELINO, *Il Regolamento Privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, p. 47.

particolare riferimento al passaggio ove viene enunciato che "è auspicabile applicare i principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile. I dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile. Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il Titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente"[164].

Pertanto, per quanto riguarda i dati pseudonimizzati[165], il GDPR già prevede la possibilità che gli stessi siano fatti rientrare nel novero della categoria di dati per i quali trova applicazione la normativa in esso dettata, e ciò allorquando, attraverso la loro combinazione con altre informazioni, siano idonei ad identificare una determinata persona[166]. Al contrario, con riferimento alle informazioni anonime, il considerando prosegue specificando che la normativa non può in questo caso trovare applicazione[167].

---

[164] Il considerando n. 26 prosegue "*Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici*". Tale disposizione va letta in combinato disposto con il considerando 30, ove si evidenzia che "*le persone fisiche possono essere associate a identificativi on line prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, marcatori temporanei (cookies), o identificativi di altro tipo, come i tag di identificazione e radiofrequenza. Tali identificativi possono rilasciare tracce che, in particolare, se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone e identificarle*".

[165] Per pseudonimizzazione si intende la conservazione dei dati in un formato tale da non identificare direttamente un individuo specifico, senza l'utilizzo di informazioni aggiuntive. Cfr. L. BOLOGNINI - C. BISTOLFI, *Pseudonymization and Impacts of Big (Personal/Anonymous) Data Processing in the Transition from the Directive 95/46/EC to the New EU General Data Protection Regulatio*n, in *Computer Law & Security Review*, 2017, p. 171 ss.; S. STALLA – A. BOURDILLON - A. KNIGHT, *Anonymous Data v. Personal Data – a False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data*, in *Wisconsin International Law Journal*, 2017, p. 284 ss.

[166] Con riferimento alla possibilità di identificazione attraverso la combinazione di più dati, il WP29 ha chiarito che non basta che vi sia la possibilità astratta di individuare una persona per considerare tale persona "identificabile" e l'informazione come "dato personale", ma che in concreto vi sia una probabilità ragionevole che l'identificazione avvenga.

[167] "[…] *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*" (Considerando 26).

Tuttavia, il dato fattuale dimostra come, stante i meccanismi di "trattamenti multipli"[168] sopra descritti, nella società contemporanea parlare di dati completamente anonimi sia un azzardo[169], data la mobile linea di demarcazione tra anonimo ed identificabile, in ragione della quale dovrebbe ritenersi percorribile l'ipotesi di estensione del raggio d'azione della normativa europea in materia di protezione dei dati personali finanche ai dati anonimi.

A sostegno di tale considerazione viene altresì in rilievo la circostanza per cui l'identificabilità cui fa riferimento l'art. 4 del GDPR comporta la possibilità di considerare identificabile la persona fisica individuabile all'interno di un contesto a prescindere che della stessa si conosca il nome anagrafico[170]: spesso, infatti, attraverso l'analisi predittiva, si può giungere alla ricostruzione del profilo di una persona specifica, senza che della stessa si conosca il nome, e tale operazione, di per sé, costituirebbe un processo di identificazione.

Inoltre, occorre tenere a mente che il dato viene qualificato "personale" anche nell'ipotesi in cui sia conosciuto solo da una cerchia determinata di soggetti, e non da tutti: in altre parole "il concetto di dato personale è assoluto, non relativo. Un'informazione o è dato personale oppure non lo è. Una volta che essa è qualificata come "dato personale" in un qualche contesto, lo è in ogni altro"[171].

Alla luce delle considerazioni svolte, occorre altresì dare atto della posizione assunta dagli organi sovranazionali. Il Parlamento Europeo, pronunciandosi in materia, ha auspicato l'applicazione delle norme europee in materia di trattamento

---

L'esclusione dei dati anonimi dal campo di applicazione della normativa europea, del resto, era già prevista dalla Dir. 95/46/Ce ed altresì dal nostro Codice *Privacy* all'art. 4.1, n) in combinato disposto con l'art. 4.1 b).

[168] L'espressione è di S. SICA, *Verso l'unificazione del diritto europeo alla protezione dei dati personali?*, in S. SICA – V. D'ANTONIO – G. M. RICCIO, op. cit., p. 5.

[169] È stato rilevato che "*it would appear therefore that no data can be entirely anonymized, and therefore all data could be considered 'personal' and therefore fall within the very strict rules of the GDP Regulation*" V. ZENO ZENCOVICH – G. GIANNONE CODIGLIONE, *Ten Legal perspectives on the "Big Data revolution"*, in *Concorrenza e Mercato*, Numero speciale, p. 34.

[170] Tale interpretazione deriva dall'orientamento consolidato dal WP29. Cfr. GPDP, 15.10.2015 [4541143], 12.3.2015 [3881392]; 8.3.2007 [1396630]; 19.11.2007 [14.45858]

[171] V. E. PELINO, op. cit., p. 53, il quale sostiene l'equipollenza, ai fini della nozione di dato personale, tra nome anagrafico e "qualsiasi elemento informativo o complesso di elementi informativi ugualmente dotati di attitudine estensiva". Già nel Parere n. 4/2007 il WP29 aveva avvertito sulla necessità di "evitare un'indebita restrizione dell'interpretazione del concetto di dati personali", proprio in virtù di una interpretazione conforme delle fonti di diritto derivato alle disposizioni dei trattati (ed in particolare all'art. 8 della Carta di Nizza), dovendosi intendere il "riferimento ai dati personali al di là dei contesti domestici e familiari".

dei dati personali[172] "al trattamento dei dati anche quando questo è preceduto da tecniche di pseudonimizzazione" ma anche ai dati del tutto anonimi, ogni qual volta il loro uso o trattamento rischi di "ripercuotersi sulla sfera privata dei singoli o su altri diritti e libertà, con la conseguente stigmatizzazione di interi gruppi di popolazione"[173]. Anche l'OCSE ha proposto una diversa definizione di dato personale, da intendersi come «qualsiasi informazione che identifica un individuo, che potrebbe essere ragionevolmente usata per identificare un individuo, o che è connessa a dati che identificano un individuo e usata in qualsiasi maniera tale da incidere su quell'individuo». Lo scopo dell'ampliamento della nozione sarebbe quello di alleviare le incertezze sulla natura "personale" o "non personale" dei dati, mettendo in evidenza il modo in cui i dati vengono usati, e la conseguenza sarebbe che «quand'anche i dati non fossero personali, essi sarebbero comunque coperti se sono connessi a, o incidono su, un individuo»[174], e ciò anche nei casi in cui non è ragionevole attendersi che il titolare del trattamento sia in concreto in grado di identificare l'interessato.

Il venir meno della distinzione tra dato personale e non personale e la possibilità di "riferirsi al dato nella maniera più inclusiva ed onnicomprensiva possibile" aumenta, tuttavia, "le difficoltà di effettiva tutela in tutti i contesti di emersione delle informazioni personali"[175], specie allorquando si faccia riferimento alla tutela predisposta nella precedente normativa, che viene comunque ripresa, nelle sue linee fondamentali, dell'attuale Regolamento.

La direttiva, infatti, che basava proprio sulla distinzione tra dato personale e non personale la tutela giuridica dell'interessato, era fondata sul modello del previo

---

[172] Ivi comprese quelle che contemplano il diritto degli interessati di ricevere informazioni riguardanti le logiche sottostanti ai processi decisionali automatizzati e alla profilazione. In tale documento, in particolare, si optava per una nozione omnicomprensiva di dato, tanto sotto il profilo della natura (potendo includere informazioni soggettive e oggettive nonché vere o false) quanto con riferimento al suo contenuto (ricomprendendo sia i dati generali sia i dati sensibili), nonché avendo riguardo al formato (non rilevando la forma cartacea, alfabetica, numerica, grafica, fotografica, acustica ovvero l'eventuale conservazione mediante codice binario). V. WP29, Parere 4/2007 sul concetto di ati personali, 20 giugno 2007, 66. Ss. Cfr. C. COLAPIETRO – A. IANNUZZI, *I princìpi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. CALIFANO – C. COLAPIETRO, Innovazione tecnologica e valore della persona, p. 104.

[173] Parlamento europeo, risoluzione 2016/2225(INI).

[174] Cfr. S. CALZOLAIO, *op. cit.*, pp. 606-607.

[175] M. GRANIERI, *Il trattamento di categorie particolari di dati personali nel reg. UE 2016/679*, in *Le nuove leggi civili commentate*, n. 1/2017, p. 165 ss.

consenso rilasciato sulla base di una precisa informativa da parte del titolare del trattamento: attualmente, però, occorre considerare che, spesso, la maggior parte dei trattamenti cui si è fatto riferimento non sono fondati sul consenso, ed ulteriormente che i titolari non sono, a volte, nelle condizioni di poter rilasciare delle informative chiare ed esaustive, specie nel caso in cui trattamenti principali di dati da loro posti in essere si combinano con molteplici trattamenti secondari.

È importante, allora, che vengano individuate delle garanzie nuove, garanzie che oggi non possono risolversi più (o non solo) nel potenziamento del "potere di controllo" dei singoli sul trattamento dei propri dati, ma che necessariamente devono coinvolgere coloro che per primi traggono beneficio dallo sfruttamento del valore di questi dati, attraverso la predisposizione di un sistema che miri a "responsabilizzare" in maniera incisiva questi ultimi.

Il Regolamento, in questo senso, nonostante tutte le limitazioni derivanti dall'incapacità di poter regolare a pieno un fenomeno tanto nuovo e tanto complesso quale quello dei *Big Data*, tenta un primo approccio ad esso attraverso la costruzione di un sistema che, seppur basato sulle tradizionali dinamiche della precedente Direttiva, cerca di superare le stesse attraverso la creazione di un modello di tutela incentrato principalmente sulla responsabilizzazione dei titolari del trattamento di dati personali, vale a dire coloro i quali, dai trattamenti in questione, sono i primi a trarre dei benefici notevoli.

3. Il mutamento di prospettiva: dalla Direttiva 95/46/CE al GDPR

La somma delle riflessioni svolte nei precedenti paragrafi circa i profondi mutamenti che il fenomeno della digitalizzazione, con ogni sua implicazione, ha indotto nella società contemporanea, ci consente ora di volgere l'attenzione alla nuova normativa in materia di protezione dei dati personali, al fine di verificare quanto il nuovo modello di tutela predisposto dal legislatore sia stato influenzato dal fenomeno di cui sopra e, ulteriormente, quanto lo stesso si sia discostato da quello precedente, delineato dalla Direttiva 95/46/CE, al fine di poterne valutare l'efficacia e l'adeguatezza rispetto alle molteplici sfide poste dall'attuale contesto sociale.

Come si è ampiamente avuto modo di evidenziare, gli strumenti normativi cui si fa riferimento sono stati varati in due momenti storici profondamente diversi.

Se, infatti, la Direttiva 95/46/CE era stata emanata al fine di regolamentare trattamenti di dati personali caratterizzati da una "dimensione relazionale binaria" o quanto meno operanti "in una sfera soggettivamente circoscrivibile"[176], ragion per cui la tutela giuridica dell'interessato rispetto al titolare del trattamento poteva fondarsi sul modello del previo consenso, rilasciato sulla base di una informativa specifica, volta a consentire il trattamento di dati *ab origine* classificabili come "personali", al contrario il Regolamento, che interviene in uno scenario totalmente differente, segnato dalla "facilitazione della circolazione delle informazioni" e dalla "crescente apertura dei mercati"[177], si occupa della regolamentazione di trattamenti che, nella maggior parte dei casi, hanno ad oggetto massicce raccolte di dati, spesso (come ampiamente evidenziato) anche di carattere non personale, che richiedono modelli di tutela ben diversi da quelli predisposti in passato.

Tali modelli di tutela si basano, in particolare, sull'implementazione di "più solide strategie di *risk assestment*, che prendano definitivamente atto del "fallimento dell'anonimizzazione" a fronte delle "reali possibilità di re-identificazione" e che considerino, pertanto, la dicotomia dato personale/dato anonimo non più idonea a garantire quel bilanciamento tra libera circolazione delle informazioni e tutela della persona[178].

L'approccio adottato dal legislatore europeo diventa dunque un "approccio incentrato sul rischio"[179], prediligendo per tale ragione un modello di

---

[176] D. POLETTI, *Comprendere il Reg. UE 2016/679: un'introduzione*, in P. PASSAGLIA – D. POLETTI, *Nodi virtuali, legami informali: Internet alla ricerca di regole*, op.cit., p. 9.

[177] *Ibidem*, p. 10.

[178] V. C. COLAPIETRO – A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, op. cit., p. 101.

[179] V. A. MANTELERO, Responsabilità e rischio nel nuovo Regolamento UE 2017/679, in Le nuove leggi civili commentate, p. 146. Cfr. altresì G. GIANNONE CODIGLIONE, *Risk based approach e trattamento dei dati personali*, in S. SICA – V. D'ANTONIO - G. M. RICCIO, op. cit., che ricorda come la tendenza ad investire i soggetti coinvolti nell'attività di trattamento dei dati di una serie di obblighi volti a promuovere l'adozione di modelli imprenditoriali ed organizzativi incentrati sulla riduzione delle ipotesi di trattamento non conforme fosse emersa già nei primi anni '80, ed altresì nel considerando 46 della Direttiva 95/46 poteva essere rintracciata una previsione in tal senso, poiché veniva messo in risalto che la tutela dell'interessato richiede l'adozione di adeguate misure tecniche ed organizzative sia nel momento della progettazione che in quello dell'esecuzione del trattamento, per garantirne la sicurezza. Cfr. altresì R. GELLERT, *Understanding the notion of risk in the General Data Protection Regulation*, in *Computer Law and Security Review*, 2018, 279 ss.

responsabilità volto alla prevenzione del danno, e non più limitato ai tradizionali aspetti concernenti la sicurezza dei dati, o alla sola dimensione individuale, ma riguardante anche gli effetti collettivi dell'uso dei dati, da cui possono conseguire diversi profili di pregiudizio.

E poiché il rischio assume, nel contesto attuale, una dimensione transnazionale[180], è importante sottolineare le conseguenze che da tale circostanza siano derivate in termini di efficacia della tutela a livello transfrontaliero.

Oggi, infatti, i dati si muovono entro una dimensione che non è più solo quella "regionale" europea, bensì quella globale caratterizzante la Rete. Il legislatore, dunque, è costretto a prendere atto del fatto che "la prescrizione di regole dettate per essere efficaci nello spazio geopolitico europeo mostra un limite intrinseco, giacché il modello europeo di regolamentazione deve necessariamente misurarsi con altri modelli che, come è noto, presentano un minor livello di protezione"[181]. Tra questi, in particolare, viene in rilievo l'ordinamento statunitense, ove si sono sviluppati i principali servizi ICT (si pensi al *cloud computing*, al *crowdsourcing*, e da ultimo ai *Big Data*): l'elemento caratterizzante tali servizi, infatti, è il fatto che gli stessi vengano erogati al di fuori del territorio in cui è stabilito il provider[182], dunque anche in Europa. Questo specifico problema è stato affrontato dal legislatore, attraverso la predisposizione di una tutela normativa che fosse, geograficamente, il più estesa possibile rispetto alla precedente Direttiva (emanata principalmente per la necessità di assicurare lo scambio a livello transfrontaliero di informazioni fra soggetti pubblici e privati dell'Unione). Tale finalità è stata realizzata attraverso la previsione dell'estensione delle disposizioni regolamentari anche ai trattamenti di dati personali effettuati da stabilimenti collocati fuori dal territorio dell'Unione europea, allorquando questi riguardino i dati personali dei cittadini europei[183].

---

[180] A. MANTELERO, op. cit., p. 147

[181] V. CUFFARO, op. cit., p. 1113.

[182] V. D. MULA, *Il trattamento dei dati nel territorio dell'Unione e il meccanismo "one stop shop"*, in S. SICA – V. D'ANTONIO - G. M. RICCIO, *op. cit.*, p. 274.

[183] Scrive al riguardo G. FINOCCHIARO "*il Regolamento affronta anche un tema geo-politico, rivendicando l'applicazione del modello europeo a livello mondiale. La legislazione europea si caratterizza per essere particolarmente rigorosa e protettiva dei diritti dell'individuo: occorrerà verificare se questo condurrà ad un'affermazione del modello europeo o invece ad un isolamento dell'Europa nel contesto globale*", in G. FINOCCHIARO, op. cit., p. 897.

Più nello specifico, l'art. 3 GDPR recita che la nuova disciplina si applica sia al "trattamento effettuato nell'ambito delle attività di uno stabilimento da parte di un Titolare del trattamento o di un Responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione", con ciò riferendosi, dunque, all'ipotesi in cui il trattamento sia effettuato da parte di uno stabilimento collocato nell'Unione, che può avere ad oggetto i dati personali tanto di cittadini europei quanto extra-europei (in ogni caso troveranno applicazione le regole del GDPR) sia al "trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un Titolare del trattamento o da un Responsabile del trattamento che non è stabilito nell'Unione" per tale intendendosi, dunque, il trattamento effettuato da parte di uno stabilimento collocato all'estero, e tuttavia relativo a dati personali "di natura europea"; in tale ultimo caso, il legislatore ha premura di precisare che il trattamento in questione deve riguardare attività di offerta di beni o servizi, oppure attività di monitoraggio dei comportamenti dei cittadini europei[184].

È soprattutto dalla previsione in esame che è possibile evincere in maniera inequivocabile l'attenzione che il legislatore ha inteso riservare all'utilizzo dei

[184] Emerge così in maniera evidente la scelta di far diventare lo "stabilimento" il parametro su cui fondare l'applicabilità della normativa. Cfr. M. G. STANZIONE, *Genesi ed ambito di applicazione*, in S. SICA – V. D'ANTONIO – G.M. RICCIO, *op. cit.*, p.27; L. BOLOGNINI - E. PELINO, *op. cit.*, p. 1 ss. Tale novità legislativa, del resto, è in linea con le più recenti pronunce della Corte di Giustizia, tra cui spicca in particolare la nota sentenza *Google Spain* (causa C-131/12), ove la Corte, nell'interpretare l'art. 4 della direttiva 95/46/CE, ritiene che ad essere rilevante per l'applicazione della normativa europea in tema di trattamento dei dati personali non è tanto il luogo in cui il trattamento dei dati viene fisicamente effettuato, quanto il luogo in cui la società che opera il trattamento esercita la propria attività. Nel caso sottoposto all'attenzione della Corte, i giudici avevano avuto modo di osservare che *Google Spain* (la cui sede legale si trova a Madrid) costituisce una filiale, sul territorio spagnolo, di *Google Inc.* (che ha sede legale negli Stati Uniti), e che la stessa vada considerata uno 'stabilimento' ai sensi della direttiva, in quanto, sebbene il trattamento dei dati personali venga effettivamente posto in essere da Google Inc., tuttavia, lo stesso viene effettuato "*nel contesto delle attività*" dello stabilimento controllato, e cioè ha luogo, ed è reso possibile, anche in virtù delle attività poste in essere dalla filiale (nel caso di specie, le attività svolte da *Google Spain* riguardavano la promozione e la vendita degli spazi pubblicitari proposti sul motore di ricerca al fine di rendere redditizio il servizio offerto da quest'ultimo). Pertanto, la Corte aveva interpretato la nozione di stabilimento in senso espansivo, al fine di ricomprendere nel raggio d'azione della disciplina in materia di trattamento dei dati personali anche quei trattamenti effettuati sì al di fuori dell'ordinamento europeo, ma anche grazie all'attività di raccolta localizzata in ambiente europeo, così da garantire una tutela più ampia possibile delle persone fisiche con riguardo al trattamento dei loro dati. Per una puntuale analisi della sentenza in esame (CGE Grande sez., 13 maggio 2014, causa C-131/12*, Google Spain, Google Inc. c. AEPD, Costeja Gonzàlez)* e di tutte le questioni giuridiche emerse, si rinvia a G. RESTA – V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, 2015.

servizi della società dell'informazione come veicolo per il trattamento di dati personali, specie ove i servizi in questione siano offerti da titolari del trattamento non residenti nel territorio europeo. Sarà compito della Commissione europea valutare poi se il paese terzo, una sua parte, o l'organizzazione internazionale destinataria dei dati garantiscono un livello di protezione adeguato[185].

Con riferimento, invece, alla necessità di una revisione dell'apparato di strumenti rimediali a tutela del singolo soggetto, come si vedrà, il legislatore è intervenuto attraverso la predisposizione di un sistema intrinsecamente complesso, riflesso della complessità dei problemi da gestire, nonché dei diversi interessi da tutelare.

4. Il GDPR: soluzione complessa per un complesso problema

L'attuale disciplina normativa è la manifestazione evidente del complesso equilibrio tra i vari interessi che il legislatore è chiamato a garantire, venuti in rilievo in un contesto sociale fortemente influenzato dai fenomeni di cui si è ampiamente fatto riferimento.

A dover essere tutelati, infatti, non sono solo i diritti e le libertà "fondamentali" aderenti al principio personalistico, e dunque i diritti e le libertà dei singoli individui coinvolti nei trattamenti di dati personali, ma, altresì, occorrerà tutelare i diritti e le libertà di matrice economica[186], che si manifestano nell'interesse alla corretta circolazione dei dati, che è un interesse di natura eterogenea, nel senso che ricomprende in sé gli interessi di una pluralità di soggetti, tra cui in particolare quelli pubblici o privati che godono di questo patrimonio informativo[187].

---

[185] Tale previsione, del resto, è conforme a quanto era stato stabilito dalla Corte di Giustizia in un altro noto caso sottoposto alla sua attenzione, anche noto come "Caso *Shrems*", ove, dopo aver ribadito la superiorità del modello europeo di protezione dei dati personali, la Corte ha invalidato la decisione di adeguatezza della Commissione adottata ai sensi dell'art. 25 della precedente direttiva per dare esecuzione nell'ordinamento all'accordo noto come Safe Harbor, concluso tra Europa e Stati Uniti. La Corte, in quell'occasione, ha affermato che spetta agli Stati nazionali valutare se gli Stati Uniti siano da considerarsi un Paese che, ai sensi della normativa in materia di protezione dei dati personali, garantisce un livello di tutela adeguato, e spetta altresì agli stesso il compito di monitorare continuativamente gli ordinamenti degli Stati terzi o delle organizzazioni internazionali che abbiano già ricevuto l'eventuale placet della Commissione. La sentenza segnalata è CGE Grande sez., 6 ottobre 2015, causa C-362/14, , *Maximilian Schrems c. Data Protection Commissioner*.

[186] V. F. BRAVO, *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tra mercato e persona: nuovi assetti nell'ordinamento europeo?*, in *Contratto e impresa*, 1/2018, p. 190.

[187] Il riferimento alla libera circolazione dei dati personali, come è stato autorevolmente evidenziato, "*funziona come una categoria teleologica e astratta: include indistintamente una*

È per tale ragione che, dapprima nell'art. 1, par. 3 del GDPR si legge che «la libertà di circolazione dei dati non può essere limitata per motivi attinenti alla protezione dei dati personali», e poi nel considerando n. 4, ove è sancito che il trattamento dei dati deve essere al servizio dell'uomo, si legge ulteriormente che «il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità»[188].

Le parole scelte dal legislatore confermano come la disciplina attuale capovolga gli equilibri del passato[189], abbandonando l'idea della protezione esclusiva, della "prerogativa assoluta" del singolo, e muovendosi piuttosto verso l'obiettivo di coniugare l'esigenza di tutela della persona con la inevitabile realtà della circolazione dei dati personali, a favore principalmente di quest'ultima[190].

---

multiforme pluralità di interessi eterogenei senza dire nulla né sulla natura dell'interesse giuridicamente rilevante espressivo dell'istanza circolatoria, né sulle ragioni della sua possibile prevalenza sulle istanze contrapposte. Analogamente alle libertà fondamentali costituenti i pilastri dell'Unione Europea, la libera circolazione dei dati personali non è un fine "ultimo" ma strumentale; è un mezzo per produrre altri mezzi per l'unico fine: il mercato unico". V. R. MESSINETTI, *Trattamento dei dati per finalità di profilazione e decisioni automatizzate*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, CEDAM, 2019, p. 168, n. 5. Altri autori hanno rilevato che "*esiste una economia dei dati (e della protezione dei dati) che si fonda […] sul trattamento, conservazione, analisi dei dati e segnatamente di dati qualificabili – all'origine o all'esito delle analisi – come personali. Questa categoria abbraccia l'intera dimensione della società dei dati e della attività di soggetti pubblici e privati, poiché è utile alla elaborazione di politiche pubbliche, così come di strategie di miglioramento del prodotto e dei servizi e di marketing aziendale e commerciale; abbraccia la profilazione della persona (o di un gruppo) non meno della relazione fra datore di lavoro e lavoratore; traccia un quadro oggettivo (e predittivo) nell'ambito del quale si possono collocare le scelte di indirizzo politico così come le decisioni che una azienda assume nei confronti di un proprio collaboratore o di un proprio potenziale cliente. Nel contesto del processo di datificazione, della società dei dati e della innovazione guidata dallo sfruttamento dei dati muta radicalmente la posizione e la funzione dei soggetti che a qualsiasi titolo svolgono attività di trattamento dei dati personali: in una parola, ne resta profondamente modificata la posizione e la funzione del titolare e del responsabile del trattamento dei dati personali*". V. S. CALZOLAIO – L. FEROLA – V. FIORILLO – E. A. ROSSI – M. TIMIANI, *La responsabilità e la sicurezza del trattamento*, in L. CALIFANO – C. COLAPIETRO, op. cit., p. 140.

[188] In dottrina si è sostenuto che lo scopo comunicativo dell'enunciato del considerando n. 4 è quello di "*rammentare agli Stati membri "recalcitranti" che pure le libertà economiche sono fondamentali e conseguentemente che i diritti e le libertà fondamentali della persona – come esistenzialità – debbono essere bilanciati con l'ordine pubblico economico europeo e le sue libertà costitutive, potendo perciò risultare occasionalmente (e ragionevolmente) sacrificati anche per le esigenze di realizzazione dell'economia digitale*". V. R. MESSINETTI, *Trattamento dei dati per finalità di profilazione e decisioni automatizzate*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, CEDAM, 2019, p. 174.

[189] F. BRAVO, *op. cit.*, p. 204.

[190] Scrive F. PIRAINO "*sotto il profilo dell'impostazione di fondo, rispetto alla dir. 95/46 il regolamento si atteggia in maniera più accentuata come una disciplina della circolazione dei dati personali, pur sensibile alle possibili conseguenze del trattamento sull'interessato, piuttosto che*

Mentre la precedente Direttiva, pur riconoscendo il valore di risorsa dei dati personali quali informazioni necessarie al funzionamento della vita economica e sociale degli Stati membri, subordinava il principio della libera circolazione degli stessi al rispetto dei diritti e delle libertà fondamentali delle persone fisiche, oggi, al contrario, il Regolamento sembra porre maggiore attenzione al profilo della "funzione sociale"[191] dei dati, in virtù del quale una eventuale restrizione del diritto individuale alla protezione dei dati personali appare legittima, nonostante il pieno riconoscimento di questo come diritto fondamentale, allorquando debbano essere garantiti altri diritti equi ordinati, propri sia dei soggetti privati che dei soggetti pubblici. Ciò, però, non significa che la tutela individuale del singolo subisca una *deminutio*: la stessa, anzi, viene rafforzata[192], ma, al tempo stesso, trascesa, divenendo uno strumento di regolazione giuridica della competizione e della concorrenza, al fine di garantire interessi collettivi di natura pubblica ed economica. La tutela del singolo, in sintesi, muove da una dimensione endogena verso una esogena[193]: il legislatore abbandona l'approccio individualista e difensivo delineato nella precedente Direttiva, a favore di un approccio che mira alla massima responsabilizzazione degli autori del trattamento.

Essendo assodato, infatti, che gli individui non sono e non possono essere del tutto consapevoli delle potenziali conseguenze del trattamento di cui i loro dati

---

come un'ulteriore tappa del lungo e accidentato percorso del riconoscimento giuridico della centralità della persona e della predisposizione di strumenti di realizzazione della personalità umana e di salvaguardia contro le interferenze esterne" in F. PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Le nuove leggi civili commentate*, 2017, p. 376.

[191] V. A. RICCI, *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, *Contratto e impresa*, 2017. L'Autrice, in particolare, spiega che "*se il dato ha uno scopo esterno alla sfera individuale dell'interessato, se il dato incide sulla sfera dei diritti fondamentali di altri individui ovvero il suo trattamento è strumentale a bisogni sociali, la pienezza delle pretese può subire una restrizione. In sintesi, se il dato personale è funzionale al soddisfacimento di un interesse che supera i confini della sfera individuale dell'interessato, legittima e necessaria è la limitazione della prerogativa sul medesimo dato. La formula della funzione sociale, ovvero della funzione nella società, si pone quindi come criterio argomentativo in cui declinare l'affermata relatività del diritto alla protezione dei dati personali. L'assolutezza del diritto alla protezione dei dati personali trova nella «funzione sociale», così come interpretata, un principio alla stregua del quale coordinare fra loro la pretesa dell'interessato, gli interessi dei* Titolari *del trattamento, le esigenze avvertite dalla società nel suo insieme*".

[192] Sempre secondo R. Messinetti, "*libera circolazione dei dati, da un lato, e protezione dei dati personali, dall'altro lato, configurerebbero istanze omogenee, correlate per una stessa finalità: tutelare la persona umana nel suo nuovo ambiente digitale; permettere la piena esplicazione della sua identità onlife*". Id., p. 171.

[193] A. MANTELERO, op. cit., p. 149.

costituiscono oggetto, è necessario che tali conseguenze siano previamente valutate da coloro che sfruttano le potenzialità dei trattamenti medesimi: ciò consentirebbe di porre i soggetti interessati nella condizione di poter assumere le proprie decisioni alla luce della valutazione dei potenziali impatti negativi che lo specifico impiego dei dati può comportare[194].

Pertanto, pur estendendo i diritti dell'interessato, e potenziando quelli già esistenti, attraverso una maggiore attenzione ai caratteri dell'informativa e all'adozione di modalità trasparenti (ai fini della formazione di un consenso realmente informato[195]), il legislatore implementa gli adempimenti in capo al titolare ed al responsabile del trattamento[196].

Del resto, le sfide della nuova era digitale non possono essere sostenute interamente dal soggetto interessato, "sovraccaricando" di significato e di efficacia il momento del consenso: di certo, tale momento è imprescindibile (allorquando il trattamento non sia fondato su altre basi giuridiche), tuttavia, da solo, non sufficiente[197]. Diviene fondamentale che, chi utilizza informazioni personali, cedute direttamente dall'interessato, ovvero ottenute sfruttando i vantaggi dei *Big Data analytics*, assuma un comportamento consapevolmente ed

---

[194] V. A MANTELERO, op. cit., p. 149.

[195] "*Il consenso dell'interessato continua ad essere il criterio di liceità del trattamento dei dati principale atteso che il modello su cui si fonda la normativa sulla protezione dei dati personali è ancora legata ad un'idea di autodeterminazione e autonomia del soggetto interessato. Risultano però fondamentali le specificazioni sul 'consenso' dirette a limitare tutte quelle soluzioni formali utilizzate per creare una fictio iuris in base a cui il soggetto interessato presta il consenso per il trattamento dei suoi dati. Viene affermato che il consenso come manifestazione dell'assenso dell'interessato al trattamento dei propri dati deve attuarsi 'mediante dichiarazione o azione positiva inequivocabile'. Al Considerando 43, viene chiarito che il consenso non costituisce il presupposto per un valido trattamento qualora vi sia un 'particolare squilibrio tra interessato e titolare del trattamento', soprattutto nei casi in cui quest'ultima sia un'autorità pubblica o comunque si possa presumere che il consenso non si sia liberamente formato. Si prevede inoltre esplicitamente che l'interessato abbia diritto di revocare il consenso in qualsiasi momento, e che il consenso possa essere revocato con la stessa facilità con cui viene accordato: non sarebbe ammissibile assoggettare la revoca del consenso da parte di un interessato a particolari formalità che potrebbero scoraggiare l'esercizio di questa facoltà. Sono previste particolari condizioni di liceità del trattamento in cui a prestare il consenso sia un minore*". V. A SPINA, op. cit.

[196] In sostanza, viene spostata l'attenzione "s*ulla struttura dei processi e dei prodotti, onde trasferire l'onere inerente la valutazione dei profili di tutela a carico di coloro che pongono in essere il trattamento, piuttosto che sull'interessato, e che si trovano quindi nella miglior posizione per adottare soluzioni tecnologiche atte a prevenire i rischi di trattamento illecito*". V. A. MANTELERO, *La riforma della Data Protection in Europa: un'opportunità per le imprese*, in *Giustiziacivile.com*, approfondimento del 03 marzo 2014.

[197] D. MESSINA, *Il Regolamento (EU) 2016/679 in materia di protezione dei dati personali alla luce della vicenda "Cambridge Analytica"*, in *Federalismi.it*, 24 ottobre 2018, p. 11.

attivamente proiettato ad un trattamento lecito dei dati a disposizione, ispirando l'intero trattamento, per tutta la sua durata, ai princìpi della protezione dei dati personali, che restano sostanzialmente immutati e vengono elencati all'art. 5: liceità, correttezza e trasparenza; limitazione delle finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

Ai titolari, dunque, vengono prescritti obblighi specifici, la cui violazione è specificamente sanzionabile ai sensi dell'art. 83 del GDPR, e ciò al fine di limitare previamente il rischio insito nei trattamenti di dati personali. La necessaria adozione di misure preventive, volte a realizzare il rispetto delle regole di trattamento ed insieme a ridurre il rischio di pregiudizi, determina una sorta di positivizzazione degli obblighi di protezione dei titolari[198].

La tradizionale prospettiva rimediale, pur essendo confermata, viene dunque ad assumere nel nuovo contesto un ruolo di chiusura del sistema, in quanto chiamata ad intervenire solo nei casi di fallimento delle soluzioni di controllo del rischio affidato al titolare. Il sistema di tutela previamente predisposto viene, cioè, completato da una politica di prevenzione del danno, in virtù della quale il titolare deve dimostrare di aver posto in essere tutte le misure idonee a prevenire lo stesso.

Assume così centralità un concetto nuovo, ricorrente nel GDPR, che è quello di *accountability*, movente dell'intera disciplina.

Si tratta di un termine mutuato dall'esperienza delle organizzazioni aziendali e societarie, che rende ancora più evidente il cambio di paradigma che ha interessato l'intero settore della protezione dei dati, divenuto ora un settore di regolazione e di *compliance* commerciale per le imprese che trattano dati, ma

---

[198] Cfr. V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali*, in *Contratto e impresa*, 2017, pp. 1115-1116. L'Autore elenca gli obblighi che il GDPR fa gravare in capo ai titolari, quali "*l'obbligo di dare avviso prontamente delle violazioni dei dati (artt. 33 e 34); l'obbligo di compiere una preventiva valutazione dei possibili rischi, anche consultando preventivamente l'autorità di controllo (artt. 35 e 36); l'obbligo di designare, in relazione a trattamenti effettuati da soggetti pubblici ovvero aventi ad oggetto particolari categorie di dati, un responsabile della protezione dei dati (art. 37), del quale il Regolamento individua (art. 39) i compiti in maniera dettagliata. A questo novero di obblighi si aggiunge poi un ulteriore complesso di regole che, sul piano volontario, prevedono l'adesione a codici di condotta elaborati autonomamente dalle associazioni di categoria (art. 40) ed ancora la eventuale sottoposizione ad un organismo di vigilanza indipendente, con procedure di certificazione delle misure adottate per la protezione dei dati, affidate ad autonomi organismi di certificazione (artt. 42 e 43) accreditati, al pari degli organismi di vigilanza, presso l'Autorità garante*".

anche un sistema di presidio dei diritti individuali, stante l'obbligatorietà di adozione di misure idonee anche in capo agli attori operanti nel settore pubblico, e non solo in quello prettamente imprenditoriale[199].

5. Il principio di *accountability* quale baricentro del nuovo sistema di protezione dei dati personali

Il Regolamento predispone un sistema di obblighi gravanti in via principale sul titolare del trattamento, e, in via gradata, sugli ulteriori soggetti attivi chiamati a collaborare con lui, e che, insieme a lui, rivestono una posizione di garanzia nei confronti dei soggetti interessati, occupandosi, a vario titolo, del trattamento dei loro dati personali. Si vuol fare riferimento non solo ai contitolari, ma anche ai responsabili del trattamento nominati dal titolare, nonché al *Data Protection Officer*, figura che, sebbene non del tutto sconosciuta nel panorama europeo, si presenta come innovativa ed indispensabile nel nuovo contesto regolamentare, poiché unica idonea a riempire di contenuto e significato quell'obbligo di protezione gravante sui titolari dei trattamenti, operando alla stregua di un "garante interno" della realtà in cui esso è nominato.

Il legislatore, dunque, estende la filiera soggettiva coinvolta nel trattamento, sebbene il titolare continui a restare il principale destinatario degli obblighi imposti dalla normativa[200].

In particolare, nel Regolamento, i titolari del trattamento diventano soggetti "a un diverso modello di compliance regolatoria, fondato su una sorta di auto-

---

[199] Cfr. V. CUFFARO, op. cit., il quale evidenzia ulteriormente che "*la disciplina europea sul trattamento dei dati personali si atteggia allora a disciplina del mercato dei dati, sollecitando a comportamenti virtuosi gli operatori del trattamento, incoraggiati a condotte coerenti con i principi di protezione in vista del conseguimento di una maggiore affidabilità agli occhi dei fornitori di dati, cioè, in definitiva, delle stesse persone i cui dati sono oggetto di trattamento. Il riferimento al mercato dei dati non intende certo dimenticare che la disciplina del trattamento tocca direttamente i valori della persona ed avverte espressamente l'esigenza di tutela delle libertà fondamentali, ma intende rimarcare che la circolazione dei dati ha ormai da tempo assunto un rilievo sul piano economico che sarebbe ingenuo se non ipocrita ignorare. Ne´ il richiamo all'idea di mercato come possibile chiave di lettura del sistema potrebbe essere inteso come un indebolimento del grado di tutela rispetto al trattamento dei dati personali, giacché nel nostro ordinamento il dettato dell'art. 41 Cost., sotto la cui egida si colloca la disciplina dell'attività economica, reca anch'esso quei riferimenti alla libertà ed alla dignità della persona che valgono sul piano assiologico a determinare la portata delle regole*".

[200] Da questo momento in poi, nell'analisi del principio di *accountability* e degli obblighi sanciti nel nuovo Regolamento, si farà riferimento esclusivamente al titolare, senza dimenticare però che gran parte dei medesimi obblighi sono previsti ulteriormente a carico del responsabile.

regolazione soggetta a controllo pubblico, che sposta su di essi oneri e incombenze di adeguamento ai parametri normativi: a tal proposito, si parla di *accountability* (art. 24) per ricomprendere con maglie abbastanza larghe la responsabilità del titolare del trattamento nel dotarsi di un robusto apparato di compliance e adottare tutte le misure tecniche e organizzative necessarie ad assicurare il rispetto della normativa sulla protezione dei dati personali"[201].

Il principio di *accountability*, come si è avuto già modo di evidenziare, sebbene appaia per la prima volta soltanto all'art. 5 GDPR[202], costituisce il perno della nuova disciplina in materia di protezione dei dati personali.

Sebbene la parola *accountability* sia stata tradotta in italiano con il termine "responsabilizzazione", da più parti è stato sostenuto come tale traduzione non possa considerarsi puntuale, poiché il termine in questione andrebbe a collocarsi, piuttosto, a metà strada tra due concetti distinti tra loro, quello di "responsabilità" e quello di "*compliance*"[203]. Dalla commistione di entrambe le nozioni deriva che per *accountability* debba intendersi, da un lato, la responsabilità, in capo al titolare, di individuare delle idonee misure di sicurezza rispetto ai rischi cui il trattamento può incorrere, e dall'altro, la capacità dello stesso di essere in grado di dimostrare, in qualsiasi momento, la propria *compliance* rispetto alla normativa di riferimento, vale a dire di rendicontare il proprio operato[204].

---

[201] A. SPINA, op. cit.

[202] L'art. 5 elenca i «princìpi applicabili al trattamento». Come sancito dal par. 1, i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato; sono raccolti per finalità determinate, esplicite e legittime, e trattati in un modo che non può essere incompatibile con tali finalità; sono conservati in una forma che consenta l'identificazione degli interessati per un tempo non superiore a quello necessario per il conseguimento delle finalità del trattamento; sono adeguati, pertinenti e limitati a quanto necessario per le finalità del trattamento; sono esatti e, se necessario, aggiornati; sono trattati in maniera da garantirne un'adeguata sicurezza e, in particolare, la protezione da trattamenti non autorizzati o illeciti, nonché dalla perdita, dalla distruzione o dal danno accidentali. L'articolo prosegue, poi, al paragrafo 2, sancendo che «*il Titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo*»: è in tale previsione che si rinviene l'origine del principio di *accountability*.

[203] La *compliance*, termine noto soprattutto nel settore imprenditoriale, esprime l'obiettivo minimo di rendere l'operato dell'impresa conforme alle prescrizioni normative. Tali prescrizioni non si limitano a minacciare gli imprenditori con sanzioni, ma mirano all'attuazione di un'efficace prevenzione endosocietaria, attraverso la concretizzazione di politiche, modelli gestionali, procedure decisionali e presidi di monitoraggio e sorveglianza che devono essere attuati all'interno delle varie realtà (in questo caso aziendali).

[204] E. L. GUASTALLA, *Privacy e Data Protection: principi generali*, in E. TOSI (a cura di), E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè, 2019, p. 83. L'obbligo di rendicontazione può essere adempiuto attraverso una serie di accorgimenti, quali ad esempio l'adesione da parte del titolare a un codice di condotta.

Tale obbligo di rendicontazione, che potrebbe essere interpretato come il derivato di un diverso e già noto principio, quello di trasparenza, che da sempre si traduce come diritto dell'interessato ad avere la completa accessibilità alle informazioni sul trattamento posto in essere da un dato operatore, nella nuova normativa assolve un fine ulteriore e diverso rispetto a quello relativo alla tutela del soggetto interessato: il titolare, infatti, dovrà sempre essere in grado di dimostrare la conformità del trattamento alla disciplina di settore[205] nei confronti di qualsiasi terzo, e particolarmente nei confronti dell'Autorità pubblica posta a presidio del rispetto del diritto alla protezione dei dati personali, fornendo la prova di aver adottato misure di sicurezza idonee a prevenire i rischi cui il trattamento è esposto. E poiché la sicurezza, nel contesto digitale contemporaneo, è intesa come "concetto dinamico e relazionale"[206], nel senso che la stessa deve essere sempre rapportata alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati personali oggetto di trattamento ed alle specifiche caratteristiche delle operazioni di trattamento da porre in essere, anche il concetto di *accountability* si presenterà, di riflesso, fortemente dinamico: il titolare non dovrà limitarsi a individuare le misure di sicurezza una volta per tutte nella fase prodromica del trattamento, ma sarà tenuto ad aggiornarle costantemente, ogni qual volta se ne presenti la necessità (magari per l'emersione di un nuovo rischio), al fine di essere considerato realmente *accountable*[207].

Per le anzidette ragioni, al titolare non verrà più richiesto di limitarsi a conformare la propria attività a criteri statici, già prefissati dal legislatore (quali ad esempio l'obbligo di adottare le c.d. misure minime di sicurezza, come avveniva nella precedente normativa), ma gli verrà demandato il più complesso compito di

---

[205] *Ibidem*.

[206] G. FINOCCHIARO, *Introduzione al Regolamento europeo*, op. cit., p. 11.

[207] Il concetto di *accountability*, dunque, presenta contenuto molto ampio. Non è un caso che spesso si sia fatto riferimento a tale concetto parlando di "*overarching concept of accountability*", ove con il termine "*overarching*" si vuol fare riferimento proprio alla portata globale dell'obbligo di responsabilità. Come si è già accuratamente considerato in altre sedi, tale obbligo di responsabilità contempla in sé:

a) l'obbligo di mettere in atto misure che rendano ogni trattamento effettuato come conforme (*compliant*) alle previsioni del GDPR;
b) l'obbligo che le misure adottate forniscano la garanzia di detta conformità;
c) l'obbligo di fondare la scelta delle misure adottate su preventive analisi dei rischi;
d) l'obbligo che la conformità così garantita sia anche facilmente dimostrabile (in primis alle Autorità di protezioni dati europee), di fatto imponendo un obbligo di rendicontazione. V. G.M. RICCIO - G. SCORZA – E. BELISARIO, *GDPR e Normativa Privacy Commentario*, *op. cit.*, p. 237.

decidere da sé le modalità e i limiti del trattamento dei dati, alla luce dei criteri guida indicati nel Regolamento[208], al fine di stimolare "un processo virtuoso e volontario che vada oltre i requisiti minimi previsti dalla legge"[209].

Si assiste, pertanto, come già anticipato, al passaggio da una visione di carattere "difensivo" della privacy, ad una di carattere "proattivo", gestionale, in virtù della quale ogni titolare modulerà la propria attività in modo da conciliare i propri scopi con la tutela del diritto fondamentale alla protezione dei dati personali. Protezione dei dati personali che, in tale contesto, viene dunque ad assumere il valore di nuovo asset aziendale, da gestire e tutelare, come si è detto, mediante modalità fortemente dinamiche, come è dinamico il rischio rispetto al quale i dati possono essere sottoposti.

Si comprende, così, la notevole importanza assunta proprio dal concetto di "rischio"[210] nel nuovo impianto normativo (non è un caso che il termine in questione ricorra appena otto volte nella direttiva ed oltre cento nel nuovo regolamento[211]): la presa di coscienza circa quanti e quali rischi siano insiti nella circolazione dei dati nell'ambiente digitale, di cui solo il titolare può fare una stima più o meno accurata prima di mettere in atto le operazioni in cui si sostanzia il trattamento, è il principale movente della revisione della normativa, ora strutturata in modo da garantire che i rischi in questione siano gestiti dai soggetti che posseggono i mezzi tecnici, giuridici ed organizzativi per farlo, attraverso la previsione di pesanti sanzioni per il caso di loro inadempimento.

---

[208] G. ARCELLA, *GDPR: il Registro delle attività di trattamento e le misure di accountability*, in *Rivista di Notariato*, 4/2018, pp. 393-398.

[209] SPINA, *op. cit.*.

[210] A. Mantelero indaga la nozione di rischio, e specifica che la stessa può essere intesa in maniera più o meno ampia. In senso ampio, il rischio consisterebbe nelle eventuali conseguenze negative derivanti dal trattamento in sé, a prescindere che lo stesso possa produrre o meno un danno o un pregiudizio ai diritti e alla libertà dei soggetti interessati. Un esempio tipico sarebbe caratterizzato dai trattamenti effettuati dai *social networks*, ove al momento dell'iscrizione l'utente dà il consenso al trattamento dei propri dati personali, esponendosi al rischio di venire profilato, ovvero monitorato a fini commerciali e quant'altro. Il trattamento in tal caso è lecito, stante il consenso prestato dall'interessato, che indicherebbe l'assunzione consapevole del rischio da parte di quest'ultimo. Tuttavia, come evidenziato dalla più recente dottrina giuridica, spesso i soggetti interessati non sono consapevoli del valore (anche economico) dei loro dati, e soprattutto non si soffermano a leggere le note informative messe a disposizione dai fornitori del servizio, consentendo pertanto agli stessi di aggirare il profilo del rischio mediante la richiesta di un consenso che nasce ab origine privo di efficacia concreta. In senso più ristretto, invece, il rischio è da intendersi quale possibilità che si verifichi un concreto pregiudizio ai diritti e alla libertà delle persone fisiche a causa del trattamento illecito dei dati personali. Cfr. A. MANTELERO, *Responsabilità e rischio nel Reg. UE 2016/679*, op. cit., pp. 153-156.

[211] S. CALZOLAIO, op. cit., p. 627.

Già in un "datato" parere del WP29, emblematicamente intitolato "Opinion 3/2010 on the principle of accountability"[212], l'Autorità aveva dichiarato che solo mediante la predisposizione di meccanismi basati sulla responsabilità i titolari del trattamento sarebbero stati incoraggiati ad attuare strumenti pratici per una protezione dei dati veramente efficace[213].

Alla luce delle sopraenunciate premesse, è possibile ora comprendere la serie di obblighi che la legge ha previsto in capo al titolare, la cui responsabilità correlata al trattamento dei dati viene accresciuta attraverso la predisposizione di un modello di gestione del rischio che si fonda, in particolare, su tre momenti, uno necessario e gli altri due eventuali: l'analisi dei rischi, la valutazione d'impatto e la eventuale consultazione preventiva della Autorità di protezione dei dati[214]. Sono, queste, tutte attività rispetto alle quali, come si vedrà, il *Data Protection Officer* ricopre un ruolo di rilievo, coadiuvando il titolare nello svolgimento delle suddette operazioni.

Il modello di gestione così predisposto, che richiama, invero, altri modelli già esistenti in settori caratterizzati da rischi elevati (ad esempio quelli di contabilità e

---

[212] Nel parere 3/2010 il WP29, dopo aver preso atto dell'evidente inadeguatezza del quadro giuridico delineato nella Direttiva 95/46/CE, che non era riuscita a garantire appieno che gli obblighi in materia di protezione dei dati si traducessero in meccanismi efficaci atti a fornire una protezione reale del diritto alla protezione degli stessi, aveva proposto alla Commissione di esaminare l'opportunità di introdurre nella normativa un principio di "responsabilità" vincolante. Si legge nel documento in questione: "*sarebbe opportuno introdurre nel quadro globale un principio di responsabilità in base al quale i responsabili del trattamento dei dati siano tenuti ad adottare le misure necessarie per garantire il rispetto degli obblighi e dei principi fondamentali dell'attuale direttiva al momento del trattamento dei dati personali. Una disposizione di questo tipo rafforzerebbe la necessità di mettere in atto politiche e meccanismi per l'attuazione efficace dei principi e degli obblighi fondamentali della direttiva attuale. Avrebbe inoltre l'obiettivo di confermare l'esigenza di adottare misure adeguate che determinino un'efficace applicazione interna degli obblighi e dei principi fondamentali attualmente stabiliti dalla direttiva. Inoltre, il principio della responsabilità imporrebbe ai responsabili del trattamento dei dati di disporre dei meccanismi interni necessari per dimostrarne la conformità agli interessati esterni, comprese le autorità nazionali di protezione dei dati. Infine, il fatto di dover dimostrare che sono state adottate misure adeguate per garantire la conformità favorirà notevolmente l'applicazione delle norme vigenti*".

[213] Così si esprime anche il Garante nelle prime istruzioni contenute nella guida on line al GDPR, consultabile all'indirizzo *https://www.garanteprivacy.it/regolamentoue/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-deidati-personali*.

[214] La dottrina ha evidenziato al riguardo che "*tutti i nuovi istituti che il Regolamento UE 2016/679 affianca alle più tradizionali – ma certamente rinvigorite - tutele sono esemplificativi di un quadro normativo lasciato dal legislatore "volutamente aperto al futuro". Questo allo scopo di ingessare il meno possibile una materia, quale quella della protezione dati, soggetta, per via della sua inestricabile connessione con la tecnologia digitale, a continue trasformazioni atte a generare sempre nuove tipologie di trattamento, in un'ottica di pianificazione e tutela dinamica, anziché statica, della protezione dei dati*". V. S. CALZOLAIO – L. FEROLA – V. FIORILLO – E. A. ROSSI – M. TIMIANI, op. cit., p. 170.

di sicurezza sul lavoro), si avvicina a quello dell'*enforced self-regulation* o della *meta-regulation*, nel senso che ai titolari viene richiesta la predisposizione, in piena autonomia, di una vera e propria *governance* interna, vale a dire sistemi di controllo e gestione dei rischi rispetto ai quali le autorità di regolazione esterna svolgono un mero ruolo di monitoraggio[215], anche in considerazione della introduzione, in molti contesti obbligatoria, della figura del *Data Protection Officer*, il quale, come si vedrà, grazie alla sua posizione nell'ambito dell'organizzazione in cui svolge le proprie funzioni, assicura che il titolare sia quanto più possibile *accountable* rispetto al dettato normativo.

E, poiché il ruolo del *Data Protection Officer*, come si anticipava, viene in rilievo particolarmente nelle attività poc'anzi richiamate, prima di passare ad una più approfondita analisi di tale figura, appare utile soffermarsi preliminarmente su queste tre fasi in cui viene a sostanziarsi in maniera più evidente il portato del principio di *accountability*.

5.1 La sicurezza del trattamento quale diretto portato del principio di *accountability* e l'analisi del rischio

L'*accountability*, o responsabilizzazione, del titolare del trattamento, si esplica, tra l'altro, se non in via principale[216], già nella fase prodromica dello stesso, attraverso l'imposizione, in capo a questi, dell'obbligo di svolgere una valutazione sistematica di tutti i rischi, attuali e potenziali, cui il trattamento, o i trattamenti, possono incorrere, al fine di individuare le misure idonee ad arginare o mitigare gli stessi. D'altronde, il titolare è il soggetto che, più di ogni altro, è in grado di conoscere a fondo la struttura e i processi organizzativi della propria organizzazione, sia essa privata o pubblica.

Nel condurre l'analisi in questione, il titolare dovrà tenere in debita considerazione sia la probabilità che si realizzino i rischi eventualmente

[215] Cfr. A. SPINA, op. cit.

[216] Il Capo IV del Regolamento, rubricato "Titolare e Responsabile del trattamento" si apre con la Sez. I rubricata "Obblighi generali". Il primo articolo della sezione in esame è il 24, che si occupa della responsabilità del Titolare del trattamento, e sancisce, come obbligo primario, quello di individuare le misure tecniche ed organizzative adeguate al fine di garantire la conformità del trattamento all'impianto normativo. Attraverso la previsione in esame, che presenta un contenuto assai ampio, il legislatore ha dunque individuato, proprio nell'obbligo in questione, il fulcro essenziale della responsabilità giuridica per il trattamento.

individuati, sia la gravità della lesione, che deriverebbe ai diritti e alle libertà delle persone fisiche, in caso di realizzazione degli stessi.

L'analisi dei rischi, pertanto, dovrà essere ispirata al criterio della massima accuratezza, specie nelle ipotesi in cui la base giuridica del trattamento non sia quella del consenso dell'interessato, bensì una delle altre previste *ex lege* (e quindi in tutti quei casi in cui il trattamento avviene a prescindere dalla volontà dell'interessato, in quanto obbligatorio *ex lege*), oppure nei casi in cui l'interessato abbia sì prestato il proprio consenso, però solo con riferimento al trattamento principale, e non anche a eventuali trattamenti secondari posti in essere dal titolare. In tale seconda ipotesi, in particolare, sul titolare graverà l'onere di tener conto del nesso esistente tra le finalità per cui i dati personali sono raccolti (in virtù del trattamento principale), e le finalità proprie del trattamento secondario, valutando in particolar modo le possibili conseguenze che il trattamento secondario può avere su quello principale.

Il legislatore, inoltre, stante la complessità che caratterizza di per sé determinati trattamenti, nonché l'inevitabile intersecarsi, nella maggior parte dei casi, di trattamenti principali con altri di carattere secondario, e considerato altresì il carattere mutevole dei rischi cui gli stessi possono essere esposti, ha previsto che l'analisi venga svolta non solo nella fase prodromica al trattamento, ma, in modo sistematico, per tutta la durata dello stesso.

L'art. 24 GDPR, infatti, che è la norma ove viene esplicato il contenuto del principio di responsabilità dei soggetti attivi del trattamento, e che inoltre costituisce la base giuridica dell'analisi dei rischi, prevede che le misure di sicurezza che il titolare individua al fine di paralizzare o arginare il rischio vengano riesaminate e aggiornate quando necessario. Anche con riferimento a tale obbligo di aggiornamento viene in rilievo il principio di *accountability*: un titolare, infatti, sarà considerato tanto più *accountable* quanto più avrà provveduto ad un riesame del rischio, con cadenze temporali precise, e ad un aggiornamento delle relative misure se necessario.

L'art. 24 GDPR prosegue specificando che "tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il

Titolare del trattamento mette in atto le misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento". Tali misure "includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del Titolare del trattamento", se ciò è proporzionato rispetto alle attività di trattamento. Con tale enunciato, il legislatore ha voluto porre l'accento proprio sul carattere di proporzionalità che caratterizza le misure in questione: tale precisazione consente di cogliere la distinzione intercorrente tra i vari trattamenti di dati personali, i quali, non essendo tutti assoggettati ai medesimi rischi (a volte addirittura a nessun rischio[217]), richiederanno misure di sicurezza di diverso impatto e proporzione.

Dalla previsione generale di cui all'art. 24 è possibile pertanto ricavare che il principio di *accountability* si esplica sostanzialmente in tre fasi principali: la prima, consistente nello svolgimento di un'analisi generale dei rischi cui il trattamento può essere esposto; la seconda, relativa all'individuazione delle misure idonee a minimizzare l'incidenza degli stessi rischi sul trattamento e dunque, *de relato*, sul diritto dei singoli alla protezione delle informazioni che li riguardano; la terza, invece, avente carattere eventuale, rappresentata dalla valutazione d'impatto ex art. 35 GDPR[218], prevista nei casi in cui i diritti e delle libertà delle persone fisiche siano esposti ad un rischio elevato.

---

[217] Con riferimento ai trattamenti che non implicano rischi elevati per l'interessato, si potrebbe fare riferimento alle indicazioni contenute nell'art. art. 27, c. 2, lett. a), dal quale è possibile ricavare che possono essere fatti rientrare in tale categoria il trattamento occasionale, ovvero quello che non abbia ad oggetto dati particolari su larga scala, o, ancora, il trattamento che, tenuto conto della natura, dell'ambito, del contesto, dell'ambito di applicazione e delle finalità dello stesso, è improbabile presenti un rischio per gli interessati.

[218] Generalmente, l'attività di analisi dei rischi è nota, nelle realtà aziendali, anche con il termine "*audit privacy*", vale a dire una valutazione, svolta da un professionista (*auditor*) in nome e per conto del titolare, che mira a far emergere le criticità riguardanti la sicurezza dei dati personali, al fine di garantire la corretta gestione dei rischi (*risk management*), i quali possono ricondotti entro due categorie: rischi di natura endogena e rischi di natura esogena. Tra i primi, quelli che più frequentemente rientrano in detta categoria sono quelli che possono derivare da eventi naturali (terremoti, incendi, inondazioni ecc.) e da errori umani (modifica, cancellazione e manomissione volontaria dei dati). Rientrano, invece, tra i rischi di natura esogena, quelli scaturenti ad esempio dal danneggiamento di *hardware* e *software* o dall'installazione di programmi *malware* etc. A seconda delle criticità riscontrate, si potranno attuare quattro diverse modalità di gestione:

- modificazione dei processi e/o modalità di gestione;
- trasferimento del rischio ad un altro soggetto;
- riduzione, attraverso processi di controllo, del livello di rischio;
- accettazione del rischio (nel caso non siano attuabili le modalità descritte ai punti precedenti).

5.2 L'individuazione delle misure di sicurezza

Con riferimento alla prima fase, si è già avuto modo di evidenziare ampiamente l'importanza della ponderazione della rischiosità del trattamento che il titolare è obbligato a condurre, e sul quale è altresì chiamato a vigilare.

In merito, invece, alla seconda fase, quella di individuazione delle misure tecniche ed organizzative adeguate, deve essere operato un richiamo a due ulteriori e diverse norme del GDPR.

La prima è rintracciabile nell'art. 32, rubricato "Sicurezza del trattamento", che apre la Sezione II, dedicata appunto alla "sicurezza dei dati personali". L'articolo richiamato, rimarcando quanto già previsto nell'art. 24, sancisce nuovamente l'obbligo per il titolare di attuare "misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio" tenendo in considerazione lo stato dell'arte e i costi di attuazione, nonché la natura, l'oggetto, il contesto e le finalità del trattamento, ed ulteriormente il rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

Tuttavia, mentre in virtù dell'art. 24 l'obbligo di adottare adeguate misure di sicurezza viene in rilievo quale mezzo utile a dimostrare l'*accountability* del titolare, al contrario, nell'art. 32, l'obbligo di predisposizione delle misure di sicurezza assume un rilievo più pregnante, poiché viene specificato che l'attuazione di tale obbligo è necessaria al fine di tutelare i soggetti interessati dal trattamento, specie in tutti quei casi in cui i rischi cui possono essere esposti i loro dati possano derivare dalla perdita, modifica, o divulgazione non autorizzata, oppure dall'accesso, in modo accidentale o illegale, ai dati trasmessi, conservati o comunque trattati.

L'art. 32 non si limita a sancire un obbligo, al contrario dell'art. 24, ma indica un vero e proprio modello di condotta ed organizzazione adeguato a garantire gli obiettivi di sicurezza, basato principalmente sulla "spersonalizzazione" dei dati,

---

Cfr. J. MAZZETTO, *L'audit privacy: i consigli pratici per individuare le criticità nella sicurezza dei dati personali*, rinvenibile al link *https://www.cybersecurity360.it/legal/privacy-dati-personali/laudit-privacy-i-consigli-pratici-per-individuare-le-criticita-nella-sicurezza-dei-dati-personali/.*

unica modalità di azione utile ad ottemperare agli standard di adeguata riservatezza e sicurezza dei sistemi di trattamento[219].

Tale "spersonalizzazione" può avvenire attraverso l'adozione di misure di diverso genere: il termine "misure", infatti, va inteso in senso lato, come qualsiasi metodo o mezzo che il titolare può impiegare per l'espletamento delle operazioni di trattamento[220]. A titolo esemplificativo, la norma indica le procedure di pseudonimizzazione e cifratura dei dati personali, nonché quelle idonee a garantire su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi di trattamento, nonché la capacità di ripristino degli stessi a seguito di incidente fisico o tecnico. Anche la procedura di revisione periodica di tali misure viene considerata di per sé una misura di sicurezza, in quanto utile al fine di testare, verificare e valutare regolarmente l'efficacia delle altre già indicate.

Ciò che è necessario, come espressamente indicato dal legislatore, è che tutte le misure prescelte siano appropriate, vale a dire idonee ai fini dell'attuazione efficace dei princìpi di protezione dei dati, riducendo i rischi di violazione dei diritti e delle libertà degli interessati: non è necessario che queste presentino un certo standard di "sofisticatezza", ma che, appunto, siano idonee rispetto al fine perseguito: il requisito di adeguatezza è, dunque, strettamente correlato a quello di efficacia[221].

---

[219] V. G. GIANNONE CODIGLIONE, *Risk based approach e trattamento dei dati personali*, in S. SICA – V. D'ANTONIO - G. M. RICCIO, op. cit., pp. 67-68.

[220] In questo senso, si assiste ad un superamento anche delle c.d. misure minime di sicurezza previste nell'allegato B del Codice Privacy italiano, poiché "*la ratio del nuovo sistema di tutela dei dati si sposta verso l'obiettivo di garantire un livello di sicurezza non astratto (come risultava essere in precedenza), bensì concreto. Tale livello di sicurezza andrà determinato in modo adeguato ad un rischio effettivo, valutato come tale dal titolare del trattamento, attraverso la scelta e l'implementazione di misure, appunto "adeguate*" a fronteggiare quel rischio specifico". V. N. BRUTTI, *Le figure soggettive delineate dal GDPR: la novità del Data Protection Officer*, in E. TOSI (a cura di), op. cit., p. 141.

[221] L'EDPS ha chiarito che con misura tecnica o organizzativa si vuol fare riferimento a qualsiasi cosa, dall'uso di soluzioni tecniche avanzate, alla formazione di base del personale incaricato a svolgere effettivamente le operazioni di trattamento, al quale potrà essere illustrato come gestire concretamente i dati dei clienti. Non è necessario, dunque, che tali misure siano "sofisticate", bensì che le stesse siano appropriate per l'attuazione efficace dei princìpi di protezione dei dati. È chiaro, inoltre, che tali princìpi potranno in qualsiasi momento, vale a dire per tutta la durata (*life-cycle*) del trattamento, richiedere che le misure in questione vengano integrate. Ad esempio, si potrebbe prevedere la possibilità per gli interessati di intervenire nel trattamento, oppure garantire loro che le informazioni circa i motivi per cui i dati personali vengono archiviati siano sempre fornite in maniera automatica. Altri esempi cui l'EDPS fa riferimento nell'indicazione delle misure adeguate sono quello relativi all'implementazione di un sistema di rilevamento *malware* su una rete di

Nella individuazione di tali misure, inoltre, il titolare dovrà tener conto dei nuovi[222] princìpi di *data protection by design* e *by default*[223], di cui all'art. 25 GDPR, rubricato, appunto, "Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita", che è la seconda norma, cui si faceva riferimento in precedenza, a venire in rilievo nell'ambito della scelta delle misure da adottare.

La norma in esame integra ed elabora tanto la previsione più generale del precedente art. 24, quanto quella del successivo art. 32, e consente di ricondurre le misure di sicurezza a due distinte categorie, ciascuna corrispondente ad un differente stadio operativo del trattamento dei dati[224]. L'art. 25, in particolare, assume notevole pregio poiché consente di porre una più accentuata attenzione sulla specifica azione che il titolare deve porre in essere con particolare riferimento alla fase di progettazione del trattamento, di cui la norma arricchisce e specifica i contenuti[225]. Infatti, la previsione *de quo*, ribadendo l'obbligo, ancora

---

computer o un sistema di archiviazione, o ancora la formazione dei dipendenti sul *phishing* o sulla "*cyber hygiene*" di base.Cfr. EDPS, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, rinvenibile al link *https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en*.

[222] In realtà, sul carattere di novità di detti princìpi, potrebbe sorgere più di un dubbio: la direttiva 95/46/CE, infatti, all'art. 17, prevedeva in capo al titolare l'obbligo di attuare misure tecniche e organizzative adeguate, al fine di garantire la protezione dei dati personali "*in caso di distruzione accidentale o illecita o perdita accidentale, alterazione, divulgazione o accesso non autorizzati*". Tale articolo, pur non facendo espresso riferimento al principio della *privacy by design*, era allo stesso tempo collegato al corrispondente considerando 46, in virtù del quale le opportune misure tecniche e organizzative avrebbero dovuto essere attuate "*sia al momento della progettazione del sistema di trattamento che del trattamento stesso*". Questa formulazione è stata ripresa dall'articolo 25 del Regolamento, che impone ai titolari del trattamento di attuare misure tecniche adeguate e misure organizzative "*al momento della determinazione dei mezzi per l'elaborazione e al momento del trattamento stesso*". Pertanto, la formulazione del GDPR non può considerarsi effettivamente innovativa, se non con riferimento alla circostanza per cui il principio sancito nella precedente direttiva viene inquadrato in un requisito legale obbligatorio, e altresì ne viene ampliato anche il campo di applicazione. Cfr. L. JASMONTAITE – I. KAMARA – G. ZANFIR-FORTUNA – S. LEUCCI*, Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR*, 4 Eur. Data Prot. L. Rev. 168 (2018).

[223] La previsione di cui all'art. 25 ha "legalizzato" i termini in questione, i quali, in occasione del Regolamento, finalmente vengono fatti uscire fuori dall'area grigia caratterizzante la categoria delle c.d. "*buzzwords*". Cfr. L. JASMONTAITE – I. KAMARA – G. ZANFIR-FORTUNA – S. LEUCCI*, op. cit.,* ove viene rilevato che "*Data Protection by Design and Data Protection by Default (DPbD and DPbDf) left the realm of 'buzzwords' and entered the one of legal obligations, once the European General Data Protection Regulation' (GDPR) was adopted in 2016*". Si tratta di "*concetti che rappresentano meglio di altri il nesso, ormai imprescindibile, esistente tra regole giuridiche e aspetti materiali e tecnologici nel campo della data protection*". V. S. CALZOLAIO – L. FEROLA – V. FIORILLO – E. A. ROSSI – M. TIMIANI, op. cit., p. 171.

[224] V. R. D'ORAZIO, *Protezione dei dati by default e by design*, in S. SICA – V. D'ANTONIO - G. M. RICCIO, op. cit., p. 80.

[225] S. CALZOLAIO, op. cit., p. 631.

una volta, per il titolare di individuare le misure tecniche e organizzative adeguate, tenendo conto dello stato dell'arte[226] e dei costi di attuazione[227] necessari per la loro applicazione, in comparazione con i caratteri strutturali del trattamento (la natura, l'ambito di applicazione, il contesto e le finalità) e con la valutazione dei rischi, stabilisce che la configurazione degli strumenti e dei metodi deve essere preordinata, sin dalla fase di progettazione del trattamento stesso (*privacy by design*), e vincolata, per tutta la sua durata, allo svolgimento di operazioni aderenti ai princìpi di protezione dei dati, ai requisiti del trattamento e alla tutela dei diritti degli interessati[228]. Il principio di *privacy by design*, dunque, implica la necessità che il prodotto o il servizio offerto tengano conto, sin dalla fase della loro progettazione, delle regole e dei princìpi della protezione dei dati, rappresentando dunque un concetto "integrato" allo stesso trattamento, al fine di renderlo sicuro[229].

[226] L'EDPS ha avuto cura di specificare, con riferimento al criterio dello "stato dell'arte", che con questo si vuol fare riferimento all'obbligo per i Titolari del trattamento di essere costantemente aggiornati circa i progressi tecnologici disponibili sul mercato, al fine di garantire una costante ed efficace attuazione dei princìpi di protezione dei dati. Si tratta di un concetto dinamico, dunque, che non può essere definito staticamente in un determinato momento, ma che varia continuamente in virtù del progresso tecnologico. In ragione di ciò, ben potrebbe il Titolare scoprire che una misura che un tempo forniva un adeguato livello di protezione, ora non è più adeguata per quel determinato trattamento. Pertanto, è necessario che i Titolari del trattamento siano costantemente aggiornati, poiché qualora trascurassero di farlo, ben potrebbe la mancata informazione essere considerata un inadempimento dell'obbligo di osservanza dell'art. 25 GDPR. Ancora, l'EDPS chiarisce che il criterio dello "stato dell'arte" non deve applicarsi solo con riferimento alle misure tecnologiche, bensì anche a quelle organizzative. La mancanza di adeguate misure organizzative, infatti, ben potrebbe diminuire o addirittura minare completamente l'efficacia di una misura tecnologica già individuata. Cfr. EDPS, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, cit.

[227] Il criterio relativo ai "costi di attuazione", invece, secondo l'EDPS, comporta l'obbligo per il Titolare di tener conto dei costi e delle risorse necessari per l'attuazione efficace e il rispetto continuo di tutti i princìpi di protezione dei dati per tutta la durata della loro elaborazione. Il costo non è inteso solo in termini di denaro o vantaggio economico, ma si riferisce alle risorse in generale, compresi il tempo e le risorse umane. Il Titolare del trattamento dovrà pianificare ed essere in grado di sostenere i costi necessari per l'efficace attuazione di tutti i principi. Questi, inoltre, non potrà far valere l'incapacità di sostenere i costi per andare esente da responsabilità. L'EDPS ha infatti chiarito che un'efficace attuazione dei princìpi non deve necessariamente comportare costi elevati: spendere tanto in tecnologie avanzate non comporta necessariamente un'attuazione più efficace dei principi di protezione dei dati. In alcuni casi, infatti, anche delle soluzioni low-cost possono essere efficaci. Cfr. EDPS, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, cit.

[228] R. D'ORAZIO, op. cit., p. 81.

[229] V. S. CALZOLAIO – L. FEROLA – V. FIORILLO – E. A. ROSSI – M. TIMIANI, op. cit., p. 173.

Al contrario, il diverso principio della *privacy by default*, di cui all'art. 25, par. 2, riguarda la necessità che il titolare ponga in essere tutte le misure tecniche e organizzative funzionali a garantire che, nel corso del trattamento, vengano utilizzati, per impostazione predefinita, esclusivamente i dati necessari alle finalità per cui questi sono stati raccolti, escludendo *ab origine* alcune tipologie di trattamento superflue o ultronee rispetto alle finalità prefissate. Tale principio sembra riproporre quanto già previsto dall'art. 5, par. 1, lett) c, relativo al più generico principio di minimizzazione (in virtù del quale la quantità dei dati raccolti nonché la durata della loro conservazione non devono eccedere il minimo necessario per le finalità perseguite), sebbene la differenza tra i due vada rintracciata nel fatto che, in virtù del principio della *privacy by default*, le misure di minimizzazione prescelte dal titolare devono essere predisposte in modo tale da garantire che la selezione dei soli dati effettivamente necessari per il trattamento avvenga grazie ad un'impostazione predefinita dei dati stessi: in sostanza, i dati devono essere "anticipatamente filtrati"[230]. Attraverso i c.d. *default settings* (le impostazioni predefinite), dunque, si mira a garantire una selezione precisa, nell'ambito delle operazioni di trattamento, dei soli dati necessari alle finalità perseguite. Ma le impostazioni predefinite mirano, altresì, a garantire che venga evitata la possibilità, ad un numero indefinito di persone fisiche, di avere accesso ai dati personali senza che vi sia l'intervento di un operatore sulla macchina (art. 25, par. 3).

In considerazione di entrambi i princìpi richiamati, è facile comprendere le critiche che la dottrina ha avanzato con riferimento alla scelta, da parte del legislatore, di individuare il solo titolare del trattamento quale unico soggetto in grado di adempiere gli obblighi di protezione fin dalla progettazione del trattamento stesso. È evidente, infatti, come l'attenzione debba essere altresì rivolta ai produttori dei prodotti, dei servizi e delle applicazioni che vengono utilizzati dai titolari, essendo, i primi, i soggetti più vicini ai dati e all'attività di elaborazione, proprio perché gli stessi forniscono al titolare i mezzi (vale a dire i prodotti e i sistemi) attraverso i quali vengono poste in essere le operazioni di trattamento. Logica vorrebbe, pertanto, che l'obbligo del rispetto dei richiamati

[230] R. D'ORAZIO, op. cit., p. 84.

princìpi venga fatto gravare, a monte, anche sui produttori, i quali dovrebbero essere tenuti a implementare le misure tecniche di sicurezza, con riferimento alle impostazioni predefinite dei prodotti o dei servizi, al fine di supportare la conformità dei titolari ai princìpi del GDPR. Lo stesso legislatore appare conscio di tale necessità, allorquando al considerando 78 specifica che "i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i Titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati". Inoltre, l'articolo 83, paragrafo 2, che stabilisce le sanzioni amministrative per l'inosservanza del regolamento, al punto d) prevede che, nel decidere l'importo dell'ammenda, le Autorità pubbliche devono considerare il grado di responsabilità del titolare del trattamento, tenendo conto delle misure tecniche e organizzative da esso attuate ai sensi degli articoli 25 e 32 GDPR.

Considerata la possibilità per il titolare di trovarsi ad operare con prodotti e sistemi già predefiniti dai loro produttori in assenza di un orientamento di *privacy by design*, ossia prodotti non pensati sin dall'origine come idonei a integrare la protezione dei dati personali, questi risponderà dell'eventuale danno anche in assenza di una sua effettiva responsabilità.

Ad ogni modo, volendosi attenere al dato testuale, è evidente come il legislatore non abbia voluto estendere l'obbligo in questione sino al punto da imporlo anche ai produttori dei servizi e prodotti, probabilmente in ragione della considerazione per cui una tale misura apparrebbe sproporzionata in un contesto quale quello tecnologico, ove imporre un sistema di responsabilità condiviso di così ampio raggio potrebbe determinare un disincentivo allo sviluppo ed agli investimenti in campo ICT[231].

Così analizzate le fasi di analisi del rischio e di individuazione delle misure di sicurezza, non resta ora che concentrarsi sull'ulteriore istituto introdotto dal Regolamento, quello della valutazione d'impatto, anche nota con l'acronimo

[231] Si pensi al caso in cui ogni titolare del trattamento, chiamato a rispondere per eventuali danni a terzi, scarichi la propria responsabilità in capo ai propri fornitori o ai consulenti, che potrebbero essere molteplici e anche trovarsi nella concreta impossibilità di andare esenti da responsabilità.

D.P.I.A., derivante dal termine inglese *Data Protection Impact Assessment*, poiché la *ratio* sottesa allo stesso altro non è che espressione dell'attenzione rivolta dal legislatore alla salvaguardia del diritto alla protezione dei dati personali nel modo più incisivo possibile, in considerazione del fatto che sono veramente numerosi i trattamenti che allo stato attuale presentano rischi molto elevati per i diritti e le libertà dei singoli, come si è avuto modo di approfondire nei primi paragrafi.

A sostegno di quanto asserito, basti considerare che il legislatore non ha previsto un elenco tassativo dei casi in cui il trattamento vada obbligatoriamente sottoposto alla valutazione d'impatto, ma piuttosto ha lasciato la possibilità, ai singoli Stati, di estendere l'elencazione contenuta nel Regolamento, e, soprattutto, ha previsto che i titolari, proprio in considerazione del principio di *accountability*, valutino da sé se vi siano le premesse necessarie per procedere a tale valutazione, dovendo eventualmente rispondere all'Autorità, in sede di controllo, in merito alle motivazioni che li hanno spinti a non darvi luogo, pur in presenza di un trattamento particolarmente pericoloso.

5.3 Il *Data Protection Impact Assessment* (D.P.I.A.)

Quando un determinato tipo di trattamento, allorché implichi in particolare l'uso di nuove ed invasive tecnologie, esponga ad un rischio particolarmente elevato i diritti e le libertà fondamentali delle persone fisiche[232], è fatto obbligo al titolare

[232] Con riferimento ai rischi "di grado elevato" cui fa riferimento l'art. 35, può essere utile operare un richiamo al considerando 75 del Regolamento, ove viene sancito che "*I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati*". In ogni caso, la circostanza per cui il rischio in questione debba essere considerato "elevato", genera diversi dubbi interpretativi, lasciando così

di sottoporre lo stesso ad una valutazione formale in merito all'impatto che può determinarsi sulla protezione dei dati personali.

L'istituto della valutazione d'impatto, disciplinato dall'art. 35 GDPR, dunque, verrà attivato dal titolare al termine della preventiva fase di analisi del rischio, allorquando questi ritenga che il trattamento continui ad essere caratterizzato da elevata rischiosità. Accanto ai casi in cui il titolare decida in via autonoma di sottoporre il trattamento alla valutazione d'impatto, ve ne sono altri in cui la stessa è imposta in via obbligatoria dal legislatore, stante la presunzione dell'elevato grado di rischiosità del trattamento che ne costituisce oggetto[233]. La lista stilata dal legislatore europeo è una lista aperta, in quanto alle Autorità di controllo degli Stati membri viene demandata la possibilità di individuare ulteriori casi in cui rendere obbligatorio il ricorso a tale istituto[234]. Alle Autorità, inoltre, viene demandata anche la possibilità di stilare una lista che elenchi i casi in cui la valutazione d'impatto non è da ritenersi obbligatoria. Con riferimento a tale previsione, la dottrina non ha mancato di evidenziare l'estrema difficoltà cui le Autorità possono incorrere nella individuazione delle ipotesi in cui un trattamento sia da considerarsi o meno particolarmente rischioso[235].

Tra le ipotesi di trattamento particolarmente rischioso, il legislatore europeo individua, nel richiamato art. 35, quelle aventi ad oggetto il monitoraggio sistematico dei comportamenti degli interessati, anche al fine di condizionarne la capacità decisionale, e quelli coinvolgenti un gran numero di soggetti su larga scala – che magari comprendano anche dati sensibili - o, ancora, i trattamenti che combinano entrambi questi fattori.

---

una discrezionalità alquanto ampia in capo al titolare in merito alla necessità di procedere o meno alla valutazione d'impatto. V. R. TORINO, *La valutazione d'impatto (Data Protection Impact Assessment)*, in V. CUFFARO – R. D'ORAZIO – V. RICCIUTO, *I dati personali nel diritto europeo*, Giappichelli, 2019.

[233] Si tratta, ad ogni modo, di una presunzione relativa, poiché dalla valutazione d'impatto svolta nel caso concreto potrebbe emergere che il rischio non è elevato come si credeva.

[234] Il Garante italiano ha sfruttato la possibilità riconosciuta dal Regolamento, e ha redatto l'elenco in questione, pubblicandolo l'11 ottobre 2018; lo stesso è rinvenibile al link *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9058979*.

[235] A. MANTELERO, op. cit., p. 157. L'autore prosegue specificando che "*sussiste una tensione fra una valutazione del rischio astratta ed a priori ed il concetto medesimo di analisi dei rischi, necessariamente incentrato sulla specificità del caso concreto. In particolare, poi, stante la possibilità di inferire dati personali ed anche sensibili partendo da informazioni di carattere non personale o non sensibile, potrebbe essere non sempre agevole presumere che, in termini generali, alcuni processi escludano in radice ogni eventualità, anche futura, di rischio elevato*".

Come è facilmente intuibile, la valutazione d'impatto sarà dunque obbligatoria non soltanto per i tanti soggetti privati che operano sul mercato ma, altresì, per tutti i soggetti pubblici che raccolgono infinite quantità di dati personali[236]. Infatti, la pericolosità di un'operazione, spesso, soprattutto nello scenario attuale, può dipendere non solo dalla natura dell'attività, ma anche dagli esiti rischiosi che questa può avere sulla collettività.

Con riferimento alla procedura utile a svolgere tale valutazione, la stessa è regolata dall'art. 35, par. 7. L'impostazione di fondo è quella della più generica analisi dei rischi, considerato che la valutazione d'impatto si pone in linea con il modello di quest'ultima, ricalcandone sostanzialmente il contenuto. Tuttavia, alcuni passaggi vengono meglio specificati. In primo luogo, infatti, il titolare, nel redigere il documento richiesto *ex lege* per tener traccia di tutta la procedura svolta, dovrà valutare *ex ante* il processo, prodotto o attività a venire in rilievo nell'ambito del trattamento, valutando il grado di rischio che da tali elementi potrebbe derivare ai diritti e alle libertà dell'interessato[237], nonché rapportando la finalità del trattamento ai princìpi di necessità e proporzionalità[238]. A questa preventiva analisi seguirà poi l'individuazione delle misure idonee ad evitare o, mitigare, i rischi individuati.

Nelle ipotesi in cui il rischio "residuale" per i diritti e le libertà degli interessati continui a presentarsi "elevato", nonostante le misure tecniche e organizzative

---

[236] Del resto, il 91° considerando precisa che costituiscono operazioni di trattamento dati su larga scala quelle in cui viene elaborata "*una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati*". I trattamenti posti in essere dai soggetti pubblici, generalmente, presentano proprio tali caratteristiche, sebbene non debba sottacersi quanto già evidenziato da Mantelero, vale a dire che "*non si coglie la ragione di adottare parametri di riferimento di carattere territoriale per qualificare il trattamento ("regionale, nazionale o sovranazionale") in relazione a processi che solitamente si pongono come slegati dai contesti territoriali, operando in ambienti cloud con una "geometria territoriale" che varia di continuo*". Cfr. A. MANTELERO, op. cit., p. 158.

[237] Nel porre in essere la valutazione d'impatto, il Titolare dovrà tener conto della differente incidenza che possono avere sul trattamento i diversi interessi e diritti degli interessati, non potendo porre sullo stesso piano i potenziali pregiudizi e vantaggi correlati al trattamento. Il Titolare, infatti, dovrà in via principale "*seguire un indirizzo volto alla mitigazione dei rischi suscettibili di incidere sui diritti fondamentali*". V. A. MANTELERO, op. cit., p. 159.

[238] Con riferimento alla valutazione della "necessità e proporzionalità" del trattamento dei dati in relazione alle finalità, occorre rilevare che, "*sebbene la valutazione non possa non prendere in considerazione le finalità del trattamento per come esplicitate al momento della raccolta dei dati, è ormai acquisito che i titolari fanno sovente un uso "trasformativo" dei dati applicando strumenti di big data analytics, rispetto a cui la valutazione di "necessità e proporzionalità" finisce per essere inevitabilmente non più corretta o comunque superata*". V. R. TORINO, op. cit, p. 869.

individuate dal titolare per mitigare l'impatto del trattamento sui diritti e le libertà degli interessati, questi dovrà procedere alla consultazione dell'Autorità di controllo, prima di dare avvio al relativo trattamento, affinché la stessa sottoponga a vaglio preventivo il trattamento in questione.

È chiaro, però, che tale processo di auto-valutazione compiuto dal titolare possa esporre a numerose falle il corretto funzionamento del sistema, e ciò sotto vari profili. A titolo esemplificativo, basti considerare il caso in cui titolare decida di dare comunque avvio al trattamento, senza passare dalla consultazione preventiva dell'Autorità, ritenendo che lo stesso non esponga i diritti e le libertà dei singoli ad un rischio di grado elevato o, alternativamente, considerando le misure di sicurezza individuate idonee ad arginare o mitigare tale rischio. Ancora, ben potrebbe verificarsi l'ipotesi in cui il titolare decida di dar luogo al trattamento, pur ritenendo lo stesso particolarmente rischioso, o pur avendo considerato le misure di sicurezza inadeguate. In questi casi, tendenzialmente giustificati da un bilanciamento costi/benefici per cui il beneficio derivante dalla messa in atto del trattamento si ritiene essere più importante dei costi che eventualmente il titolare sarebbe costretto a sostenere in sede di controllo successivo (e, dunque, in sede di responsabilità), determinerebbe un serio pericolo per la salvaguardia del diritto alla protezione dei dati personali degli interessati. Questi, infatti, saranno costretti a poter agire solo *ex post* nei confronti del titolare, una volta che si sia verificato l'eventuale danno, ma non sarà garantita loro alcuna efficace tutela preventiva.

Se il titolare pone in essere il trattamento nella consapevolezza di non avere adottato le misure adeguate ad arginare determinati rischi, e se lo fa – altresì - nonostante l'eventuale parere discordante del *Data Protection Officer*[239], posto che quest'ultimo non può avere alcun potere impeditivo nei suoi confronti né alcun obbligo di segnalazione nei confronti dell'Autorità, è chiaro che il suo operato negligente andrà a determinare delle ricadute importanti sull'intero sistema di tutela predisposto dal legislatore.

Ancora, occorre ulteriormente ribadire, e la dottrina non manca di farlo, nel tentativo di evidenziare ulteriori criticità proprie dell'istituto della valutazione d'impatto, sebbene di carattere applicativo, che la prassi invalsa, nell'epoca dei

[239] Sul rapporto tra Titolare e DPO nell'ambito del D.P.I.A. si tornerà nel Capitolo IV, ove verranno altresì sviluppate le riflessioni appena esposte in ordine alle scelte compiute dal titolare.

Big Data, di accumulo e combinazione secondaria dei dati previamente raccolti rende problematico per il titolare tener conto dell'uso trasformativo che di detti dati può venir fatto da titolari successivi cui vengano ceduti i pattern di dati. Per tale ragione, la dottrina ritiene che l'istituto della valutazione d'impatto vada implementato affinché la stessa possa concentrarsi sull'impiego concreto che il titolare intenda fare dei dati, specie nel caso in cui questi siano oggetto di cessione ad altri soggetti, e ciò al fine precipuo di fornire all'interessato, anche nelle more del trattamento, le opportune informazioni circa i rischi, ma anche circa le garanzie offerte[240].

Aldilà delle considerazioni svolte, occorre rilevare che il WP29 si è espresso favorevolmente in merito a tale istituto. Il Gruppo di lavoro ha, infatti, emanato delle linee guida in materia[241], ove viene evidenziato che la valutazione d'impatto "costituisce una buona prassi al di là dei requisiti di legge, poiché attraverso di essa il Titolare può ricavare indicazioni importanti e utili a prevenire incidenti futuri. In questo senso, la valutazione di impatto permette di realizzare concretamente l'altro fondamentale principio fissato nel regolamento 2016/679, ossia la protezione dei dati fin dalla fase di progettazione (data protection by design) di qualsiasi trattamento".

6. Verso un'*accountability* condivisa?

L'analisi delle disposizioni normative relative ai più innovativi obblighi che, ai sensi della nuova normativa, gravano in via principale sul titolare del trattamento, e in via secondaria sugli altri soggetti attivi, e che discendono direttamente dal principio di *accountability*, ha permesso di mettere in risalto la dimensione, assai ampia, che tale principio assume nel nuovo contesto normativo, dato che la sua efficacia non si esaurisce al momento dell'adozione delle misure idonee a fronteggiare i rischi e garantire la sicurezza del trattamento, ma richiede, ulteriormente, agli autori del trattamento, la capacità di dimostrare in qualsiasi

[240] A. MANTELERO, op. cit., pp. 160-161.

[241] Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01), 13.10.2017, rinvenibili al link https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

momento la conformità delle attività poste in essere al dettato legislativo[242]. Tale conformità si realizza pienamente nel momento in cui gli autori dei trattamenti adempiono correttamente agli obblighi previsti *ex lege*, i quali hanno varia portata e complessità.

È chiaro che, al fine di adempiere correttamente a quanto imposto dal dettato legislativo, e al fine, più pregnante, di realizzare, in una prospettiva di efficienza funzionale oltre che economica, le necessarie strategie e misure di *accountability*, gli autori del trattamento non potranno agire da soli, ma dovranno necessariamente essere coadiuvati da altri soggetti. Del resto, è evidente come non si possa assolutamente pretendere che, tanto nel settore privato quanto in quello pubblico, coloro che ricoprono cariche dirigenziali abbiano tutte le competenze utili a far fronte ai numerosi adempimenti privacy richiesti *ex lege*, anche in considerazione del fatto che, spesso, tali adempimenti presentano delle notevoli difficoltà di attuazione dal punto di vista pratico.

È per tale ragione che il legislatore ha previsto una ristrutturazione precisa dell'organigramma dei soggetti attivi deputati al trattamento dei dati personali. Si tratta di una scelta coerente con l'innovativo approccio che caratterizza l'intera disciplina, ispirato a criteri di *project management*[243]: una volta determinato l'obiettivo da raggiungere, è necessario costruire un modello operativo *ad hoc*, che coinvolga i diversi operatori dedicati al trattamento dei dati personali, delineando con precisione ruoli e incarichi di ciascuno. È evidente infatti che, se la protezione dei dati personali entra a far parte integrante dei valori condivisi di una certa organizzazione, la stessa debba necessariamente essere strutturata in modo che le responsabilità siano ripartite, con precisione, fra i diversi soggetti che concorrono al trattamento, e che l'azione di ciascuno di loro sia indirizzata al rispetto di quel principio di *accountability* che, sebbene sembri essere stato pensato quale criterio

---

[242] M. GAMBINI, *Principio di responsabilità e tutela aquiliana dei dati personali*, *Quaderni della Rassegna di diritto civile diretta da Pietro Perlingieri*, *Edizioni Scientifiche Italiane*, 2018, p. 8.

[243] Come messo in luce da attenta dottrina "*l'impianto complessivo del GDPR tradisce una struttura complessa, ispirata alle strutture articolate delle grandi imprese, nazionali e multinazionali, in cui si può agevolmente osservare il principio di segregation of duties fra le varie figure soggettive della filiera privacy (Titolare, Responsabile, DPO) e si possono investire ingenti budget e risorse umane all'adempimento dei nuovi precetti sia sotto il profilo organizzativo che della sicurezza dei dati*". V. E. TOSI, *Privacy digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo Codice Privacy*", in E. TOSI (a cura di), op. cit., p. 18.

ispiratore principalmente dell'azione del solo titolare del trattamento (e degli altri soggetti, nei casi espressamente indicati), in verità assume una portata "espansiva", proprio perché lo stesso coinvolge, anche solo in via indiretta, tutti i soggetti che gravitano nell'organizzazione del titolare.

Con riferimento a quest'ultimo, proprio al fine di favorire un approccio a tale principio, da parte sua, non timoroso ma proattivo, il legislatore ha introdotto, come obbligatoria, tanto nelle realtà pubbliche quanto nei settori privati che si occupano di determinate tipologie di trattamento, una figura, terza ed indipendente, che lo coadiuvi in qualità di organo di supporto: il *Data Protection Officer*.

Da più parti è stato evidenziato come questa figura costituisca una delle novità più rilevanti dell'intero impianto normativo, in termini di misure tecniche e giuridiche di *enforcement* delle *policy* di *data protection*. Tuttavia, come si avrà modo di indagare nel prossimo capitolo, il legislatore ha scelto di non dedicare un sistema di regole completo con riferimento a questa nuova figura professionale, limitandosi piuttosto ad indicarne ruolo e funzioni, e lasciando indeterminati tutta una serie di profili che avrebbero, viceversa, meritato una maggiore considerazione, primi fra tutti la qualificazione professionale e l'individuazione di un sistema di regole di responsabilità in relazione alla posizione assunta nei confronti del titolare e, più in generale, della sua organizzazione (sia essa pubblica o privata), nonché nei confronti di eventuali altre categorie di soggetti con i quali potrebbe venire in rapporto nello svolgimento dei propri compiti e funzioni.

Nel prossimo capitolo si analizzeranno più approfonditamente le disposizioni normative espressamente dedicate a tale figura, e si metteranno in luce i tanti interrogativi cui tali disposizioni lasciano spazio, i quali non sembrano destinati a trovare risposta nel periodo immediato.

CAPITOLO TERZO
IL *DATA PROTECTION OFFICER* NEL REGOLAMENTO (UE) 2016/679

1. Il *Data Protection Officer* nella fenomenologia dei soggetti attivi del trattamento

Tra le misure di nuova portata che il legislatore europeo ha introdotto al fine di attuare e concretizzare il principio di *accountability*, ve n'è una che assume una rilevanza più pregnante delle altre: si tratta dell'introduzione del *Data Protection Officer* (conosciuto anche con l'acronimo anglofono DPO), tradotto in Italia con il termine Responsabile della Protezione dei Dati Personali (RPD).

Il DPO è una figura professionale di carattere innovativo, dotata di caratteristiche e funzioni peculiari, che allarga il novero dei soggetti attivi del trattamento, andando ad affiancarsi agli altri principali attori già noti, vale a dire il titolare, gli eventuali contitolari, il responsabile, e gli incaricati. Tuttavia, l'utilizzo del termine "affiancamento" alle figure soggettive indicate non deve dar luogo a fraintendimenti, soprattutto in riferimento alle funzioni ed al ruolo che il DPO assume.

Facendo riferimento all'intero quadro soggettivo del sistema del trattamento dei dati personali, infatti, possiamo immaginare un cerchio diviso in tre aree: in una prima andranno a collocarsi il titolare (con gli eventuali altri contitolari), ed il responsabile; in una seconda, i soggetti passivi, vale a dire gli interessati; da ultimo, nella terza, l'Autorità pubblica di controllo (in Italia rappresentata dal Garante per la protezione dei dati personali).

Ebbene, nel tentativo di una collocazione sistematica, si ritiene che il DPO non dovrebbe essere inserito direttamente nell'area alla quale afferisce il titolare, né in nessuna delle altre: piuttosto, appare opportuno ipotizzare una quarta area, posta centralmente, che inferisce con ciascuna delle tre aree circostanti: egli, infatti, si presenta come "figura di raccordo" sia tra i soggetti attivi del trattamento e gli interessati, sia tra i primi e l'Autorità Garante[244].

[244] V. F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, op. cit., p. 109.

Data la funzione di "catalizzatore" per l'insieme dei processi indispensabili per garantire un'adeguata attuazione dei requisiti del GDPR[245], il suo ruolo viene in rilievo, in modalità trasversale, sotto un duplice profilo di interesse: da un lato, la nomina del DPO rappresenta di per sé l'attuazione di una misura di garanzia di natura organizzativa da parte del titolare[246], e dall'altro lato, l'operato del DPO funge da garante e promotore della *compliance* del titolare nei confronti dei terzi, siano essi gli interessati o l'Autorità di controllo[247].

Emerge così il doppio significato da attribuire a tale funzione: se da un lato, infatti, il DPO viene nominato dal titolare nell'ambito della propria organizzazione per non incorrere in eventuali sanzioni o in responsabilità per il caso di mancata nomina, e dunque per dimostrarsi *accountable (*e questo sembrerebbe il significato principale della figura, secondo il tenore letterale delle norme), dall'altro, in virtù della sua funzione di collaboratore del titolare, il DPO ne garantisce la conformità dell'operato ai princìpi del GDPR. In particolare, proprio con riferimento alla tutela dei dati personali degli interessati, la presenza del DPO nell'azienda o nell'ente dovrebbe essere considerata quale ulteriore ed idonea garanzia circa la predisposizione, a livello organizzativo e strutturale, di adeguate ed idonee misure di sicurezza rispetto alle attività di trattamento poste in essere.

Come si avrà modo di evidenziare, secondo alcuni studiosi, proprio in ragione di tale seconda funzione, il DPO potrebbe essere assimilato alle autorità regolatorie indipendenti: da una tale equiparazione deriverebbe che l'interesse protetto da tale figura non debba considerarsi solo quello privato del titolare, come sembrerebbe emergere dal dato testuale, ma anche quello di natura generale, cioè di carattere superindividuale alla liceità del trattamento ed alla correttezza dei rapporti giuridici.

---

[245] R. MARTINEZ, *El delegado de protecciòn de datos, in A. RALLO LOMBARTE (a cura di), Tratado de protecciòn de datos: actualizado con la Ley Organicà 3/2018, de 5 de diciembre, de proteccion de datos personales y garantìa de los derechos digitales*, Tirant lo Blanch, 2019, p. 433.

[246] C. SOLINAS, *La nuova figura del responsabile della protezione dei dati*, in V. CUFFARO – R. D'ORAZIO – V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, op. cit., p. 882.

[247] N. BRUTTI, *Le figure soggettive delineate dal GDPR: la novità del Data Protection Officer*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, op. cit., p. 149.

A tal riguardo, sebbene necessario punto di partenza non possa che essere il dato testuale, non appare da escludere, sia in considerazione delle ragioni che hanno caratterizzato l'evoluzione della disciplina in merito, sia in considerazione dell'obbligo di cooperazione con l'Autorità pubblica (che la legge indica espressamente tra i compiti propri del DPO), una possibile rivisitazione del ruolo in esame, seguendo peraltro itinerari interpretativi già sperimentati in passato rispetto ad altri organi e funzioni di controllo, originariamente concepiti a servizio dell'interesse privato e che nel tempo sono state re-interpretate con l'affidamento di mansioni di stampo pubblicistico[248].

Prima di ripercorrere l'*excursus* che ha interessato tale figura nelle esperienze precedenti al GDPR, occorre fare una doverosa premessa. Sebbene, *prima facie*, la definizione italiana di "responsabile della protezione dei dati personali" possa ingenerare confusione nell'interprete nazionale dal punto di vista terminologico, poiché la stessa potrebbe essere confusa con quella di "responsabile del trattamento di dati personali" (prevista dall'art. 4 comma 1, lett. g) del D. Lgs. 196/2003), e nonostante, in passato, alcuni compiti che la nuova normativa attribuisce oggi al DPO siano stati svolti proprio dal responsabile del trattamento, in verità si tratta di figure profondamente diverse[249]. Nello specifico, il DPO,

[248] A titolo esemplificativo, si può citare il collegio sindacale, nato come organo di controllo del consiglio di amministrazione per conto dell'assemblea, al quale sono state assegnate, soprattutto dalla legislazione speciale, compiti di garanzia verso il mercato e le autorità regolatorie.

[249] L' Autorità Garante per la Protezione dei Dati Personali nel 2015, ha pubblicato una relazione ove definisce la traduzione italiana del termine una scelta "un pò infelice". Nella stessa Relazione si legge che al DPO "*saranno affidati compiti sostanziali, per assicurare il rispetto della normativa in materia di privacy da parte della società o ente nell'ambito del quale viene designato. Sarà affidato a questo nuovo soggetto, dotato di una specifica professionalità nel settore della protezione dei dati personali, il ruolo di "presidio avanzato" del rispetto dei principi e degli adempimenti in materia nonché di interlocutore ed elemento di connessione tra il titolare del trattamento e l'Autorità*". La Relazione è reperibile all'indirizzo *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5204513*. Cfr., con riferimento al confronto tra le due figure, G. M. RICCIO, *Data Protection Officer e altre figure*, in S. SICA – V. D'ANTONIO – G. M. RICCIO, *La nuova disciplina europea della privacy*, CEDAM, 2016, ove viene dato atto di due differenze principali. La prima, e più rilevante, risiede nella configurazione stessa del ruolo del DPO, il quale si caratterizza per essere una figura di alta professionalità che agisce in qualità di "supervisore" *autonomo* e *indipendente* dell'attività del Titolare del trattamento dei dati, e ciò a prescindere dalla sua collocazione nell'organigramma dell'ente: la legge, infatti, prevede che possa essere nominato DPO sia un soggetto esterno all'amministrazione o azienda, sia un lavoratore già alle dipendenze del Titolare del trattamento. Al contrario, il Responsabile del trattamento, si caratterizza per essere un dipendente del Titolare, agendo per suo conto e sottostando alle decisioni strategiche di esclusiva competenza di quest'ultimo, le quali spesso, peraltro, vengono adottate a seguito di un confronto proprio con il DPO. La seconda distinzione intercorrente tra i due organi risiede nella disciplina inerente la loro

sebbene agisca in qualità di soggetto designato dal titolare (sia che adempia le sue funzioni in virtù di un contratto di servizi, e dunque da esterno rispetto alla realtà del titolare, sia che le svolga in ragione di un atto di designazione, se già suo dipendente) non è tenuto, contrariamente al responsabile, ad adempiere ad obblighi etero-imposti dal titolare, essendo assicurata allo stesso la piena autonomia e indipendenza rispetto a quest'ultimo. Sul punto, infatti, appare opportuno sottolineare come il DPO, in ragione della sua qualificata professionalità, ha come compito principale quello di supportare nonché controllare l'attività del titolare, ed anche quella del responsabile del trattamento, nell'assolvimento degli obblighi loro imposti *ex lege*, non dovendo sottostare alle loro direttive.

2. Le origini del *Data Protection Officer* tra Europa e Stati Uniti

Il DPO, sebbene rappresenti senz'ombra di dubbio una novità di rilievo nella nuova disciplina normativa (ci si potrebbe azzardare a definirla la novità più importante), in verità non è una figura del tutto sconosciuta nell'ambito del panorama legislativo europeo, dal momento che questo ruolo era già stato oggetto di normazione negli ordinamenti di alcuni Stati membri. In particolare, il legislatore pare essersi ispirato, nella redazione degli articoli del Regolamento dedicati, principalmente alla disciplina tedesca: sono numerose, infatti, le analogie con la figura del *datenschutzbeauftragter*, il cui ruolo era stato oggetto di disciplina sin dal 1977 [250].

Oltre a quella prevista nell'ordinamento tedesco, una figura embrionale di DPO poteva già essere rintracciata nella Direttiva 95/46/CE, nota come "*Data Protection Official*": tuttavia, stante il carattere non vincolante dello strumento

---

nomina: mentre la nomina del DPO (salvo determinate eccezioni) è prevista come obbligatoria *ex lege*; al contrario, con riferimento all'incarico del Responsabile del trattamento, l'opportunità della nomina rientra nelle scelte di auto-organizzazione del Titolare, ammettendosi la possibilità che questi non abbia alcuna necessità di avvalersi di un responsabile, sebbene al giorno d'oggi sia estremamente raro non aver bisogno di almeno un responsabile per lo svolgimento di determinate operazioni legate al trattamento (si pensi, ad esempio, alla necessità di avvalersi di un servizio di *cloud storage* per l'archiviazione dei dati: generalmente, tale servizio è gestito da soggetti esterni alla compagine organizzativa del titolare del trattamento, i quali verranno considerati quali responsabili del trattamento nel momento in cui il Titolare proceda all'acquisto di detto servizio).

[250] Per una disamina della disciplina normativa inerente il DPO nell'ordinamento tedesco si rinvia al par. 5.

normativo scelto dal legislatore, non tutti gli Stati membri avevano deciso di avvalersi della possibilità di prevedere tale figura nell'ambito dei loro ordinamenti, ed è per questa ragione che per molti di loro, Italia compresa, la stessa costituisce una vera e propria novità[251].

Anche negli ambienti extra-UE è possibile rintracciare una figura per molti versi simile al DPO, il "*Chief Privacy Officer*", soggetto venuto in rilievo, per la prima volta, nel 1999, anno in cui è stata istituita la società *All Advantage*, specializzata in servizi pubblicitari offerti tramite Internet: la società aveva nominato l'avvocato Ray Everett Church primo *Chief Privacy Officer* degli USA, ossia dirigente del settore aziendale della *privacy* [252]. Da quel momento in poi, la posizione di *Chief Privacy Officer*, ed altre posizioni similari legate alla gestione della *privacy*, si erano diffuse al punto da dar luogo alla nascita di varie associazioni di categoria, tra le quali spicca, la I.A.P.P. (*International Association of Privacy Professionals*), che costituisce oggi la più nota organizzazione internazionale di professionisti della *privacy*, con più di 20.000 professionisti associati in 83 nazioni.

Lo *Chief Privacy Officer* viene considerato, negli Stati Uniti, una figura strategica di gestione, che lavora in cooperazione con altri dirigenti di "*C-level*"[253] ed è chiamato a garantire che le grandi società americane tutelino i consumatori rispetto all'utilizzo che viene fatto dei dati personali da parte delle aziende, nonché al fine di coadiuvare gli imprenditori per una gestione tanto efficace quanto conforme alle norme inerenti il tema della sicurezza dei dati personali.

Allo stato attuale, la figura del DPO, così come delineata dal GDPR, presenta evidenti analogie con quella del *Chief Privacy Officer* americano, sebbene la profonda differenza intercorrente tra la normativa europea e quella americana a

---

[251] Si rinvia al par. 3.

[252] In un'intervista rilasciata da Chruch, questi ha dichiarato "*quando nel 1999 sono stato nominato Chief Privacy Officer il mio ruolo è stato il primo nel suo genere: una posizione di dirigente con il compito di vigilare su tutte le questioni legate alla privacy*". S. Comellini, in verità, riferisce che il primo incarico di *Privacy* Officer in USA era stato affidato a Jennifer Barrett Glasgow, designata dalla Acxiom Corporation nel 1991. V. S. COMELLINI, *Il Responsabile della Protezione dei Dati (Data Protection Officer – DPO)*, in *Soluzioni di Diritto* (direzione scientifica di N. GRAZIANO), Maggioli Editore, 2018, p. 22.

[253] In particolare, si fa riferimento agli *Chief* (dirigenti) le cui aree di interesse si sovrappongono a quella del *Privacy* Officer, vale a dire il *Chief Information Officer* (CIO), il *Chief Security Officer* (CSO), il *Chief Data Officer* (CDO) e il *Chief Compliance Officer* (CCO)

tutela dei dati personali incida anche sul differente tipo di presidio che le figure "garanti" di *C. Privacy Officer* e DPO sono chiamate a svolgere.

3. Il *Data Protection Official* nella Direttiva 95/46/CE

Come già anticipato, il ruolo del DPO rappresenta solo in parte una novità nel panorama legislativo, proprio perché una figura embrionale dello stesso può essere rintracciata già nella precedente Direttiva 95/46/CE [254].

La Direttiva, infatti, dopo aver definito all'art. 2 il ruolo dei soggetti attivi del trattamento, quali il "*controller*"[255] ed il "*processor*"[256], nella traduzione italiana rispettivamente "titolare del trattamento" e "incaricato del trattamento"[257], all'art. 18 e al successivo art. 20, faceva riferimento a questa ulteriore figura, il "Data Protection Official", di cui, tuttavia, non veniva offerta alcuna definizione, né negli articoli in questione, né nello stesso art. 2, che pure si occupava di offrire una definizione di tutti i soggetti a vario titolo implicati nelle attività di trattamento.

L'art. 18, nel prevedere in capo al titolare l'obbligo preventivo di notificare all'Autorità di controllo ogni trattamento o insieme di trattamenti da svolgere[258], stabiliva altresì la possibilità, per gli Stati membri, di esonerare quest'ultimo da tale onere al ricorrere di determinate circostanze.

---

[254] Nella Relazione alla proposta di Regolamento è scritto che l'istituto "si basa sull'articolo 18, paragrafo 2, della direttiva 95/46/CE che ha permesso agli Stati membri di introdurre tale obbligo in sostituzione di un obbligo generale di notificazione".

[255] Dir. 95/46/CE, art. 2, lett. d): *"controller" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law*.

[256] Dir. 95/46/CE, art. 2, lett. e): *"processor" shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.*

[257] Nel trasporre la Direttiva 95/46/CE nell'ordinamento nazionale, la Legge n. 675/1996, poi confermata dal D. lgs. n. 196/2003, ha distinto i soggetti attivi in titolare, responsabile e incaricato (le rispettive definizioni potevano essere rintracciate all'art. 4 comma 1, lett. f), g) ed h) del D. Lgs. n.196/2003): il titolare del trattamento è colui che, nella Direttiva, era identificato con il termine "*controller*", mentre il termine "*processor*" è stato tradotto come "incaricato", vale a dire l'operatore tecnico. Nel nostro ordinamento è stata prevista poi, a parte, un'ulteriore figura, quella del responsabile, che identificava il soggetto preposto dal titolare a trattare dati personali per conto di quest'ultimo. Cfr. G. M. RICCIO, *op. cit*.

[258] Come spiega il quarantottesimo «considerando» della direttiva, «*la notificazione all'autorità di controllo ha lo scopo di dare pubblicità alle finalità del trattamento ed alle sue principali caratteristiche, per consentirne il controllo secondo le norme nazionali di attuazione della [suddetta] direttiva*».

La prima riguardava il caso in cui i trattamenti da porre in essere, in considerazione dei dati che ne costituivano oggetto, non fossero tali da poter arrecare un pregiudizio ai diritti e alle libertà delle persone interessate[259]; la seconda, invece, riguardava il caso in cui il titolare del trattamento avesse designato, in maniera conforme alla legislazione nazionale applicabile, un *Data Protection Official*, ruolo che, nella traduzione italiana era stato indicato come "incaricato della protezione dei dati"[260].

Il compito precipuo di tale figura consisteva nell'assicurare, in maniera indipendente, l'applicazione nell'ambito dell'organizzazione aziendale, delle disposizioni nazionali di attuazione della direttiva ed altresì di tenere un registro dei trattamenti effettuati dal titolare del trattamento[261].

---

[259] Nel recepire la direttiva, il nostro legislatore aveva previsto, all'art. 7 della L. 675/1996, l'obbligo di notificazione preventiva da parte del Titolare per tutti i tipi di trattamento posti in essere. Successivamente, a seguito della modifica intervenuta ai sensi dell'art. 3, D. lgs. n. 476/2001, il legislatore aveva stabilito che la notificazione fosse dovuta solo in casi predeterminati *ex lege*. Ai sensi dell'art. 37, c. 1 del Codice *Privacy*, oggi abrogato, era stato previsto che la notificazione fosse obbligatoria per i trattamenti aventi ad oggetto:
a) dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;
b) dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;
c) dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;
d) dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;
e) dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;
f) dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.
Era previsto inoltre che tale elencazione potesse altresì essere ampliata dal Garante con provvedimento *ad hoc*, in caso di individuazione di trattamenti potenzialmente dannosi e idonei a ledere i diritti e le libertà degli interessati.

[260] Si noti al riguardo come la parola "*official*" è stata tradotta in italiano come "incaricato", mentre al contrario, l'odierno "*officer*" è tradotto come "responsabile".

[261] La Corte di giustizia dell'Unione europea (CGUE) ha avuto l'opportunità di offrire un chiarimento con riferimento all'art. 18 par. 2 della Direttiva 95/46 / CE, nel caso *Volker und Markus Schecke and Eifert*. Il caso, alquanto complesso, aveva determinato il giudice del rinvio a chiedere – tra le altre - un'interpretazione autentica relativamente all'onere del *Data Protection Official* di tenere un «registro dei trattamenti effettuati dal Titolare del trattamento in cui figurino le informazioni di cui all'articolo 21, par. 2, della direttiva 95/46». Nella sentenza, la CGUE, dopo aver sottolineato che il DPO ha una serie di compiti volti a garantire "*che le operazioni di trattamento non abbiano effetti negativi sui diritti e le libertà delle persone interessate*", ha evidenziato che l'art. 18, par. 2 non impone all'incaricato alla protezione dei dati personali di

Accanto alla previsione di cui all'art. 18, la Direttiva conteneva un ulteriore richiamo alla figura del *Data Protection Official* all'art. 20, ove veniva sancito che i trattamenti che potevano presentare, potenzialmente, rischi specifici per i diritti e le libertà delle persone, dovevano essere obbligatoriamente esaminati prima della loro messa in opera, e che tali verifiche dovessero essere effettuate o dall'Autorità pubblica di controllo, una volta ricevuta la notifica da parte del titolare, oppure dalla persona incaricata della protezione dei dati (il *Data Protection Official*) il quale, in caso di dubbio circa l'elevata rischiosità degli stessi, avrebbe dovuto, in ogni caso, consultare l'Autorità.

Dalla lettura del combinato disposto dell'art. 18 e dell'art. 20 emerge dunque che, sebbene il legislatore europeo avesse stabilito, in via generale, l'obbligo per ogni titolare di notificare previamente al Garante ogni trattamento da porre in essere (a prescindere dalla base giuridica dello stesso, e ricomprendendo, dunque, tanto i trattamenti svolti per finalità di lucro dai soggetti privati, generalmente basati sul consenso, quanto quelli svolti dai soggetti pubblici per l'offerta di un servizio di interesse pubblico, basati dunque sulla natura più generale e superindividuale dell'interesse stesso), tuttavia questi aveva comunque concesso agli Stati la possibilità di esonerare i titolari da tale obbligo, al ricorrere di due eccezioni: la prima, relativa ai casi di trattamenti di dati personali non sottoposti a rischi particolari; la seconda, invece, che si sarebbe verificata allorquando i legislatori nazionali avessero imposto ai Titolari l'obbligo di avvalersi di un soggetto interno alla propria organizzazione, idoneo a garantire la conformità del loro operato al dettato legislativo. Nel caso, poi, che i trattamenti fossero stati esposti a rischi particolarmente elevati, l'incaricato in questione sarebbe stato comunque tenuto a consultare l'Autorità ai fini del rilascio di un parere preventivo.

Ne deriva che, in caso di trattamenti non rischiosi, il legislatore avesse previsto la possibilità, per gli Stati, di esimere il titolare non solo dall'obbligo di notifica

---

tenere un registro prima che sia effettivamente realizzato il trattamento di dati da parte del Titolare del trattamento. Infatti, il registro in questione, deve contenere solo i trattamenti che siano concretamente posti in essere dal Titolare. *Case-92/09 Volker und Markus Schecke and Eifert (CJEU, 9 November 2010) ECLI:EU:C:2010:662, par. 98-99*. In merito all'obbligo di tenuta del registro, occorre sin d'ora evidenziare che lo stesso obbligo si può oggi rintracciare nel GDPR, all'art. 30. Tuttavia, nella nuova normativa, tale obbligo viene fatto gravare sul Titolare del trattamento, sebbene non sia da escludere che, nella prassi, sia proprio il DPO ad adempiervi, specie nelle realtà di dimensioni medio-piccole.

preventiva, ma anche da quello di nomina del *Data Protection Official,* posto che tale nomina era ritenuta essenziale solo nell'eventuale caso di trattamenti con un certo indice di rischio, in considerazione dell'impatto sociale che questi potevano avere sui diritti e libertà delle persone fisiche interessate.

Per contro, la nomina del *Data Protection Official* avrebbe consentito ai titolari, pur occupandosi di trattamenti di dati personali esposti a particolari rischi, di non dover provvedere alla notificazione all'Autorità di controllo, riducendo così anche gli adempimenti burocratici di quest'ultima.

L'Autorità, infatti, a seguito di ogni notificazione, aveva sempre l'obbligo di procedere al controllo volto a verificare la corrispondenza dei trattamenti alle previsioni legislative o regolamentari, nonché di tenere il relativo registro in cui andavano iscritte le notificazioni dei titolari[262].

In presenza di nomina dell'incaricato alla protezione dei dati, invece, l'Autorità sarebbe dovuta intervenire solo nel caso in cui il trattamento fosse stato esposto ad un rischio particolarmente elevato, ovvero in tutti gli altri casi in cui se ne fosse ravvisata la necessità: tale valutazione, relativa alla rischiosità del trattamento, sarebbe stata svolta o dal titolare o dallo stesso *Data Protection Official*, poiché, come rilevato, la notifica di cui all'art. 20 poteva essere autonomamente effettuata da quest'ultimo.

La *ratio* del sistema così predisposto dal legislatore europeo nella Direttiva non sembra discostarsi del tutto da quella che, a distanza di un ventennio, ha animato la redazione delle norme del GDPR riferite al DPO: ciò che muta trai due testi, essenzialmente, è che, in passato, la scelta di introdurre o meno tale figura era stata lasciata alla discrezionalità degli Stati, oggi invece la stessa è stata prevista come obbligatoria in tutti i casi espressamente indicati dal Regolamento. Inoltre, se in passato la previsione di tale figura era stata percepita essenzialmente come un modo per evitare il controllo preventivo e a tappeto da parte dell'Autorità per

[262] Si trattava di un mero procedimento dichiarativo, vale a dire rientrante nel novero di quei procedimenti volti a determinare un fatto di conoscibilità di altro fatto (l'esistenza di un trattamento), onde fornire un ulteriore strumento di controllo ai soggetti interessati, che in qualsiasi momento avrebbero potuto verificare quali trattamenti dei loro dati fossero in corso. Si trattava, dunque, di un mero adempimento formale, avente carattere di utilità solo nei confronti dei soggetti interessati dal trattamento, che potevano così esercitare un controllo sulla quantità e tipologia di trattamenti effettuati dai titolari del trattamento con i loro dati.

ogni trattamento, oggi la sua previsione assume un significato più pregnante quale riflesso del principio di *accountability* che ispira l'intera normativa.

La disciplina del Data Protection Offical, dunque, sembra anticipare in parte quella dell'odierno DPO, e ciò appare chiaro guardando ai compiti che la Direttiva attribuiva a questi, sebbene in modo molto generico: la tenuta del registro delle attività di trattamento (che, tra l'altro, nell'odierna disciplina è considerato un compito del Titolare ex art. 30 GDPR, sebbene spesso venga affidato da quest'ultimo al DPO) ed il controllo sulla conformità dei trattamenti al dettato legislativo, con la possibilità di consultare l'Autorità pubblica nei casi particolarmente rischiosi. Oggi, invece, le disposizioni del GDPR dedicate al DPO contengono svariate indicazioni ultronee, e ne delineano funzioni e compiti che caratterizzano in modo indefettibile lo *status* del DPO, a garanzia della sua autonomia ed indipendenza e della sua competenza professionale, come si avrà modo di analizzare nel prosieguo delle presenti considerazioni[263].

3.1 La relazione della Commissione sull'applicazione della Direttiva 95/46/CE, con particolare riguardo all'art. 18 ed il report del WP29

Sull'applicazione della Direttiva 95/46/CE - ed in particolare, per quanto di rilievo in questa trattazione - dell'art. 18 da parte degli Stati Membri, la Commissione europea si era pronunciata, in data 15 marzo del 2003, con la "*Prima relazione sull'applicazione della direttiva sulla tutela dei dati 95/46/CE*"[264].

L'organo esecutivo dell'Unione Europea, dopo aver dato atto delle differenze esistenti nelle disposizioni nazionali di attuazione della Direttiva e di un generale ritardo nell'attuazione della stessa da parte di alcuni Paesi membri[265], aveva dato

[263] C. SALINAS, op. cit., p. 890.

[264] (COM (2003) 265 — C5-0375/2003 — 2003/2153(INI)). Tale relazione è stata redatta in virtù di quanto previsto dalla Direttiva 95/46/CE all'art. 33, ossia l'obbligo per la Commissione di presentare periodicamente al Parlamento europeo ed al Consiglio una relazione sull'applicazione della direttiva, accompagnata, se del caso, dalle opportune proposte di modifica.

[265] Nonostante la possibilità offerta dall'art. 18 della Direttiva di essere esonerati dall'obbligo di notifica preventiva all'Autorità, è curioso notare come siano stati soltanto cinque gli Stati membri che si sono serviti di tale esenzione, attraverso la previsione della nomina del *Data Protection Official*: Germania, Paesi Bassi, Svezia, Lussemburgo e Francia. Tuttavia, mentre in Germania tale nomina era stata sin da subito prevista come obbligatoria per i soggetti pubblici nonché per quelli privati con più di quattro persone impiegate nel trattamento automatizzato di dati, al contrario in Svezia, Francia e Lussemburgo la stessa era solo facoltativa. Cfr. G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli, 2016, p. 89.

rilievo alla circostanza per cui "da più parti è stata sostenuta la necessità di una semplificazione e di un ravvicinamento delle disposizioni adottate dagli Stati membri per quanto riguarda la notificazione delle attività di trattamento da parte dei responsabili del trattamento".

La Commissione, pur condividendo la necessità di una semplificazione normativa in merito agli obblighi di notificazione, aveva colto l'occasione per rimarcare la possibilità offerta agli Stati di esentare i titolari dall'obbligo in questione, attraverso la previsione della nomina del *Data Protection Official*. In particolare, la Commissione aveva evidenziato che tale deroga "consente una sufficiente flessibilità pur senza inficiare il livello di protezione assicurata", invitando così tutti gli Stati ad un uso più ampio della stessa.

Nella parte conclusiva della relazione, la Commissione aveva poi fatto appello al WP29, al fine dell'avanzamento di proposte intese a semplificare, in maniera sostanziale, gli obblighi in materia di notificazione negli Stati membri, specie da parte delle multinazionali con stabilimenti in diversi Paesi.

Cogliendo le sollecitazioni della Commissione, il WP29, in data 18 gennaio 2005, aveva redatto un report "*on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the Data Protection Officers in the European Union*"[266].

Dopo aver evidenziato che nel 2002, in occasione della revisione della Direttiva 95/46/CE, i rappresentanti delle grandi imprese operanti nel mercato digitale avevano manifestato la necessità di una modifica della disciplina relativa agli obblighi di notifica, nella parte in cui prevedeva che gli stessi effettuassero tante notifiche per quanti fossero gli stabilimenti presenti nei diversi Stati membri, il WP29 ha provveduto ad individuare gli strumenti utili per semplificare il sistema di notificazione[267], e, con riferimento alla figura dell'incaricato alla protezione dei

---

[266] Rinvenibile al link *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp106_en.pdf.*

[267] Di seguito si riportano le quattro possibili strategie suggerite dal WP29 per semplificare l'onere di notificazione:

1. Justification that a notification has been completed in one Member State, as a prerequisite to apply for a simplified procedure.

2. Similar processing operations would be a must. Processing operations in the country where the notification took place and in the country where the simplified system is being used should be very similar. Using the same information system, for example, would help the applicant to demonstrate the existence of similar processing operations.

dati (al quale nel *report* ci si riferisce per la prima volta appellandolo "*Data Protection Officer*" e non più "official"), ne ha raccomandato un più ampio ricorso, principalmente nelle aziende che si occupano di determinati settori industriali (senza però specificare quali) nonché nelle grandi organizzazioni pubbliche. L'Autorità ha poi avuto cura di chiarire che la nomina in questione non avrebbe determinato la riduzione delle informazioni accessibili alle Autorità di controllo, laddove tali informazioni si fossero rese necessarie, né avrebbe determinato l'automatico venir meno degli obblighi di notifica nei confronti delle suddette Autorità, stante la necessità di dovervi obbligatoriamente procedere in caso di trattamenti particolarmente rischiosi. Inoltre, il WP29 ha altresì evidenziato l'ulteriore scopo di tale nomina, come strumento di semplificazione e sgravio per le Autorità pubbliche, che in tal modo avrebbero potuto concentrarsi su altri trattamenti o settori con maggiori probabilità di pregiudicare la *privacy* degli individui.

In sostanza, la lettura interpretativa fornita dal WP29 sembra confermare quanto già evidenziato in precedenza, e cioè che, attraverso la nomina di un incaricato alla protezione dei dati, si sarebbe venuto a realizzare il passaggio da un supervisore esterno (l'Autorità di controllo) ad uno interno (il DPO), dotato delle funzioni di garanzia e vigilanza tipiche dell'Autorità.

4. Il *Data Protection Officer* nel Regolamento 2001/45/CE [268]

Ulteriore importante momento nell'evoluzione della figura del DPO è quello inerente la previsione dello stesso nell'ambito del Regolamento 2001/45/CE, relativo ai trattamenti di dati personali posti in essere dalle istituzioni e dagli

---

3. The provision of information to other data protection authorities (by means of model fiche translated into all official languages) would be limited to the content of Article 19 of the Directive + 3: time of data storage, information on the sources of the data and mechanisms made available to data subjects to exercise their rights. Compliance with national law may also require identification of data transfers or prior checkings.

4. Data Protection Authorities may, on a case-by-case basis, request the provision of additional information, if the provision of such additional information was deemed necessary in attention to the particular circumstances of the case at hand.

[268] 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*", recentemente oggetto di revisione (la versione aggiornata è rinvenibile al link *https://edps.europa.eu/sites/edp/files/publication/18-09-30_dpo_position_paper_en.pdf*).

organismi comunitari[269]. Ai sensi del Regolamento in esame, su tali istituzioni e organismi, per i quali non è previsto l'obbligo di notifica preventiva dei trattamenti di dati personali al Garante Europeo per la Protezione dei Dati (anche conosciuto con l'acronimo EDPS – *European Data Protection Supervisor*) [270], salvo il caso di trattamenti particolarmente rischiosi, grava, un vero e proprio *obbligo* (e non più una mera facoltà) di designazione del *Data Protection Officer*[271].

In riferimento alla obbligatorietà di tale nomina deve considerarsi che, stante l'inesistenza dell'obbligo di notifica del trattamento per i titolari in questione, il legislatore europeo abbia ritenuto opportuno, in via alternativa, prevedere che gli stessi si dotassero di un DPO deputato a svolgere l'attività di controllo (preventivo) che sarebbe toccata all'Autorità pubblica; accanto a questa prima e più immediata giustificazione, tuttavia, la stessa obbligatorietà potrebbe celare un significato più profondo.

I trattamenti in questione, infatti, sono posti in essere da soggetti pubblici, vale a dire soggetti che svolgono le loro funzioni per il perseguimento di un interesse pubblico, sicché la necessità di un controllo preventivo da parte di un'Autorità esterna potrebbe rivelarsi privo di utilità, in considerazione della finalità dei

[269] Le istituzioni e gli organismi comunitari sono definiti "*controller*", termine anche stavolta tradotto in italiano come "Titolare". Ai sensi dell'art. 2 del Regolamento 2001/45/CE, il "*controller*" è "l'istituzione o l'organismo della Comunità, la direzione generale, l'unità o qualunque altra entità organizzativa che, singolarmente o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali. Quando le finalità e i mezzi del trattamento sono determinati da un atto comunitario specifico, il titolare del trattamento o i criteri specifici per la sua designazione possono essere fissati da tale atto comunitario".

[270] Il Garante europeo della Protezione dei Dati, istituito nel 2001, in applicazione dell'art. 286 del TUE e dell'art. 42 del Regolamento 2001/45/CE del Parlamento europeo e del Consiglio, ha il compito di garantire il rispetto dei diritti e delle libertà fondamentali delle persone fisiche riguardo al trattamento dei dati personali posti in essere dalle istituzioni e dagli organismi comunitari. Nell'ambito della sua attività, può produrre tre tipi di documento: attraverso i "*position paper*" offre una interpretazione autentica su argomenti di propria competenza; i "*background paper*" sono pareri o raccomandazioni sul miglior modo di agire, e vengono rilasciati a seguito dello sviluppo di una analisi preventiva o particolarmente approfondita; i "*policy paper*", infine, vengono stilati allorquando il Garante voglia comunicare le proprie determinazioni circa il modo in cui intende agire rispetto ad un problema specifico oppure in linea generale.

[271] Il legislatore non utilizza più l'espressione "*Data Protection Official*" di cui al precedente (e, all'epoca, ancora vigente) art. 18 della Direttiva 95/46, ma quella di "*Data Protection Officer*", anticipando così la dicitura oggi nota. Altresì, viene a mutare la traduzione italiana del termine, in quanto lo stesso non viene tradotto come "incaricato", ma come "Responsabile della protezione dei dati personali", esattamente come avviene oggi con riferimento al DPO previsto dal GDPR. Tuttavia, occorre rilevare che anche nel Regolamento 2001/45/CE, così come nella Direttiva 95/46/CE, manca la definizione di DPO, sia nelle norme in cui ne vengono disciplinati compiti e funzioni, sia nella norma dedicata alla spiegazione delle definizioni ricorrenti nel testo legislativo.

trattamenti di dati personali, inerenti e funzionali al perseguimento di quel bene pubblico cui l'attività di tali soggetti è indirizzata e che, pertanto potrebbe giustificare anche attività di trattamento di dati personali con alto indice di rischio per i diritti e le libertà delle persone fisiche.

Ciò giustifica, da un lato, la scelta del legislatore europeo di non prevedere l'obbligo di notifica in capo a tali soggetti, e dunque di eliminare il controllo preventivo dell'Autorità; a fronte di tale situazione, tuttavia, apparrebbe di dubbia utilità l'obbligo, imposto agli stessi, di dotarsi di un "controllore interno", se questi venisse considerato alla stregua di controllore della mera conformità delle attività di trattamento al dettato legislativo.

Ma è proprio su questo profilo che viene in rilievo il vero significato della funzione del DPO, soprattutto in ambito pubblico: la nomina di tale soggetto, infatti, non viene in rilievo come misura alternativa all'assenza dell'obbligo di notifica, e dunque di un controllo preventivo dell'Autorità, stante il carattere "necessario" e "obbligatorio" del trattamento, giustificato dall'interesse pubblico perseguito dalle istituzioni, quanto piuttosto come misura idonea a garantire che il diritto alla protezione dei dati personali degli interessati venga tutelato (da parte del titolare/ente pubblico) nel migliore dei modi possibili, attraverso l'adozione di tutte le misure idonee a evitare o mitigare le probabilità che possano verificarsi illeciti ed incorrere in sanzioni.

In caso di trattamenti posti in essere dai soggetti pubblici, proprio il profilo dell'obbligatorietà correlata all'interesse pubblico, che prescinde dalla scelta del titolare di assumere il rischio del trattamento per interesse proprio, come avviene nel settore privato, evidenzia come l'attività del DPO serva sì a rendere il titolare *accountable* rispetto alla legge, ma soprattutto, ed essenzialmente, sia necessaria al fine di garantire gli standard ottimali ed i massimi livelli di protezione dei dati personali degli interessati, proprio in tutti quei contesti in cui il trattamento non venga posto in essere in ragione della manifestazione del loro consenso.

I trattamenti in questione, proprio perché necessari e obbligatori, anche in ipotesi di alto indice di rischio, richiedono un controllo incisivo, che deve essere effettuato da parte di un soggetto competente e che sia inserito nella struttura dell'ente, e dunque in grado di poter svolgere continuativamente il suo ruolo per

garantire al meglio gli interessati e gli eventuali soggetti terzi a diverso titolo (eventualmente) coinvolti.

Il pregio del Regolamento 2001/45/CE è indubbiamente quello di aver resa manifesta la necessità che tutti i soggetti pubblici, indistintamente, e dunque a prescindere dal servizio svolto, stante l'enorme quantitativo di dati raccolti e la possibilità di circolazione e scambio di tali dati, si avvalgano obbligatoriamente di un DPO, che consenta agli stessi di predisporre delle misure di sicurezza idonee a garantire la tutela del diritto alla protezione dei dati personali e verificare la persistenza degli standard di sicurezza.

Le norme del Regolamento 2001/45/CE che disciplinano la funzione e i compiti del DPO nelle istituzioni ed organismi comunitari sono state in gran parte riprese dal legislatore europeo nel GDPR, in considerazione del fatto che tali norme avevano approfondito il contenuto della funzione del DPO, oltrepassando gli angusti limiti dei due enunciati dell'art. 18 della Direttiva 95/46/CE con riferimento al *Data Protection Official*.

La disciplina inerente il DPO delle istituzioni europee è contenuta negli artt. 24-26 del Regolamento 2001/45/CE. Più precisamente, l'obbligo di nomina e l'elenco delle funzioni assegnate a tale figura sono disciplinati all'art. 24[272]; il

[272] Regolamento 2001/45/CE, art. 24 "*Nomina e mandato del responsabile della protezione dei dati*":
1. Ogni istituzione ed organismo della Comunità nomina almeno un responsabile della protezione dei dati personali con il mandato di:
a) garantire che i responsabili del trattamento e gli interessati siano informati dei propri diritti ed obblighi ai sensi del presente regolamento;
b) rispondere alle richieste del garante europeo della protezione dei dati e, nell'ambito delle sue competenze, cooperare con il garante europeo della protezione dei dati su richiesta di quest'ultimo o di propria iniziativa;
c) garantire in maniera indipendente che le disposizioni del presente regolamento vengano applicate all'interno dell'istituzione o organismo di cui fa parte;
d) tenere il registro delle operazioni effettuate dal responsabile del trattamento, riportandovi le informazioni di cui all'articolo 25, paragrafo 2;
e) notificare al garante europeo della protezione dei dati i trattamenti che possono presentare rischi specifici ai sensi dell'articolo 27.
Il responsabile garantisce in tal modo che i trattamenti non arrechino pregiudizio ai diritti e alle libertà degli interessati.
2. Il responsabile della protezione dei dati è scelto in funzione delle sue qualità personali e professionali e, in particolare, delle sue conoscenze specifiche in materia di protezione dei dati.
3. La scelta del responsabile della protezione dei dati non deve dar luogo a un possibile conflitto di interessi tra la sua funzione di responsabile ed altre eventuali funzioni di ufficio, in particolare nell'ambito dell'applicazione delle disposizioni del presente regolamento.
4. Il responsabile della protezione dei dati è nominato per un periodo da due a cinque anni. Il suo mandato è rinnovabile; la durata complessiva del mandato non può superare i dieci anni. Può

successivo art. 25 si occupa dell'obbligo di notificazione al DPO, da parte dell'istituzione o organismo, di tutti i trattamenti di dati personali posti in essere, affinché questi ne prenda nota in un registro[273], il cui obbligo di tenuta è previsto dall'art. 26, che disciplina altresì il contenuto dello stesso[274], ricalcando quanto previsto dalla Direttiva[275].

Ciò che preme mettere in risalto, in relazione alla disciplina in esame, è l'insieme delle disposizioni dedicate al rapporto intercorrente tra il DPO ed il Garante europeo.

---

essere destituito dalle sue funzioni di responsabile della protezione dei dati dall'istituzione o organismo comunitario che lo ha nominato solo con il consenso del garante europeo della protezione dei dati, se non soddisfa più le condizioni richieste per l'esercizio delle sue funzioni.
5. La nomina del responsabile della protezione dei dati è comunicata al garante europeo della protezione dei dati dall'istituzione o dall'organismo comunitario che lo ha nominato.
6. Il responsabile della protezione dei dati ottiene dall'istituzione o dall'organismo comunitario che lo ha nominato il personale e le risorse necessarie all'esercizio delle sue funzioni.
7. Il responsabile della protezione dei dati non può ricevere alcuna istruzione per quanto riguarda l'esercizio delle sue funzioni.
8. Altre norme d'attuazione relative al responsabile della protezione dei dati sono adottate da ogni istituzione o organismo della Comunità nel rispetto delle disposizioni che figurano nell'allegato. Tali norme d'attuazione potranno in particolare riguardare le funzioni, gli obblighi e le competenze del responsabile della protezione dei dati."

[273] Regolamento 2001/45/CE, art. 25 "*Notificazione al responsabile della protezione dei dati*":
1. Prima di eseguire uno o più trattamenti dei dati, destinati al conseguimento di una o più finalità correlate, il responsabile del trattamento ne informa il responsabile della protezione dei dati.
2. Le informazioni da fornire includono:
a) il nome e l'indirizzo del responsabile del trattamento e l'indicazione dei servizi di un'istituzione o un organismo incaricati del trattamento di dati personali per una particolare finalità;
b) la finalità o le finalità del trattamento;
c) una descrizione della categoria o delle categorie di interessati e dei pertinenti dati o categorie di dati;
d) il fondamento giuridico del trattamento al quale sono destinati i dati;
e) i destinatari o le categorie di destinatari ai quali possono essere comunicati i dati;
f) un'indicazione generale dei termini ultimi per bloccare e cancellare le diverse categorie di dati;
g) i trasferimenti di dati previsti verso paesi terzi o organizzazioni internazionali;
h) una descrizione generale che consenta una prima valutazione dell'adeguatezza delle misure adottate in forza dell'articolo 22 per garantire la sicurezza del trattamento.
3. Il responsabile della protezione dei dati deve essere informato senza indugio di ogni modifica relativa alle informazioni di cui al paragrafo 2."

[274] Regolamento 2001/45/CE, art. 26 "*Registro*":
"*Ogni responsabile della protezione dei dati tiene un registro dei trattamenti notificati a norma dell'articolo 25.*
Il registro riporta almeno le informazioni di cui all'articolo 25, paragrafo 2, lettere da a) a g). Il registro può essere consultato da chiunque direttamente o indirettamente tramite il garante europeo della protezione dei dati."

[275] Il registro, in particolare, costituisce un importante strumento, utile a garantire una efficace forma oggettiva di trasparenza, considerato che gli interessati "*possono trovare presso ogni ente comunitario uno o più centri di riferimento per conoscere non solo se siano in corso trattamenti di loro dati e quali, ma anche puntuali e significative notizie sui caratteri di ogni trattamento*". V. P. PALLARO, *Libertà della persona e trattamento dei dati personali nell'Unione Europea,* Giuffré, 2002 p. 244.

Dalla lettura delle norme dedicate emerge, infatti, come tale rapporto si caratterizzi, in particolar modo, per la stretta collaborazione che intercorre tra i due. Il DPO, in particolare, è tenuto a rispondere a tutte le richieste formulate dall'Autorità e a cooperare con questa, su richiesta di quest'ultima o di sua iniziativa. Inoltre, sarà suo onere, e non del titolare, valutare quali trattamenti siano da considerarsi particolarmente rischiosi e così procedere (di sua iniziativa) alla notifica all'Autorità, al fine di un controllo preventivo da parte di quest'ultima. In ultimo, la disposizione che più di ogni altra incide in modo significativo sul rapporto in questione (oltre che sulla configurazione stessa del ruolo del DPO), è quella contenuta nell'art. 24, n. 4, ove non solo viene sancito che la durata del mandato del DPO è temporalmente limitata (in un periodo compreso tra due e cinque anni, con la possibilità di rinnovo, salvo che non si superino i dieci anni complessivi), ma viene altresì previsto che, nel caso in cui l'istituzione o organismo vogliano destituire il DPO, perché questi non soddisfa più le condizioni richieste per l'esercizio delle sue funzioni, è necessario il preventivo consenso del Garante europeo. Proprio questa necessità di un previo consenso denota, ancora una volta, l'atipicità del ruolo in esame che, pur configurandosi come lavorativo/fiduciario con l'ente che lo ha nominato, risente di una ingerenza esterna, da parte di un'Autorità di controllo pubblica, in grado di incidere direttamente sul rapporto tra titolare e DPO. Questo profilo si presenta di indubbio interesse e sarà richiamato anche nelle pagine seguenti, dedicate all'analisi della figura del DPO nell'ambito del GDPR.

Accanto alla disciplina presente negli artt. 24-26, il Regolamento 2001/45/CE dedica al DPO un intero allegato, ove viene specificato che, oltre l'esercizio delle funzioni elencate dall'art. 24, a questi viene attribuito anche il compito di formulare raccomandazioni, all'istituzione o all'organismo comunitario che lo ha nominato, per il miglioramento delle misure e delle *policies* di protezione dei dati, nonché, ancora, il compito di svolgere una funzione consultiva tanto nei confronti della istituzione o dell'organismo, quanto nei confronti di qualsiasi soggetto lo richieda, per chiarire eventuali criticità circa l'applicazione delle disposizioni sulla protezione dei dati. Ancora, può svolgere indagini, di propria iniziativa o su

richiesta, su questioni e fatti collegati all'esercizio delle sue funzioni, e riferire in merito al soggetto che lo ha incaricato dell'indagine e/o al titolare del trattamento.
Il DPO, inoltre, deve avere accesso in qualsiasi momento ai dati oggetto del trattamento, a tutti gli uffici, ed ai supporti informatici ove i dati sono contenuti. Infine, viene rimarcato l'obbligo di riservatezza di cui all'art. 287 del TFUE rispetto alle informazioni e ai documenti di cui il DPO sia venuto a conoscenza nell'esercizio delle sue funzioni.

4.1 Il "*Position Paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001*"

Il Regolamento, proprio per la parte riguardante la previsione della nomina del DPO, è stato oggetto di interpretazione autentica da parte dell'EDPS, che il 28 novembre 2005 ha pubblicato un "*position paper*" indirizzato all'analisi di tale ruolo nell'ambito delle organizzazioni europee. Nel documento, intitolato "*Position Paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001*"[276], l'EDPS ha colto l'occasione per ribadire quanto sia rilevante nell'organigramma delle istituzioni e degli organismi europei il ruolo giocato dal DPO, stante la funzione di garanzia a questi assegnata in merito al rispetto dei princìpi e delle disposizioni del Regolamento in materia di trattamento dei dati personali. Proprio in considerazione del rilievo di tale figura, spiega l'EDPS, è necessario che ogni istituzione o organismo nomini "almeno" un DPO[277], specificando, tuttavia, che la nomina in questione non implica di per sé la conformità dell'operato delle istituzioni alle disposizioni del Regolamento. È necessario, altresì, che le stesse collaborino attivamente con il DPO: facendo riferimento all'esperienza maturata in più di quattro anni di applicazione del Regolamento, l'EDPS sottolineava come spesso le istituzioni fossero venute meno, ad esempio, all'obbligo di notifica al DPO di ogni trattamento posto in essere, derivando da tale circostanza il grave problema della conseguente

[276] Rinvenibile al link: *https://edps.europa.eu/sites/edp/files/publication/05-11-28_dpo_paper_en.pdf*.
[277] Il Garante europeo dà atto della necessità che, in alcune istituzioni, sia presente anche un assistente del DPO, ed in altre persino di un "DPO coordinatore", con il compito di coordinare tutti gli aspetti relativi alla protezione dei dati nei vari uffici in cui si possono articolare le direzioni.

mancata notifica per il (necessario) previo controllo da parte del Garante Europeo, ai sensi dell'art. 27, per tutti i trattamenti particolarmente rischiosi.

L'EDPS prosegue, ulteriormente, soffermandosi sul requisito dell'indipendenza del DPO e sui modi attraverso i quali la stessa può essere garantita. A tal proposito, rileva come non possa essere considerato indipendente il DPO *part-time*, vale a dire il soggetto, già lavoratore dipendente dell'istituzione, che svolga più incarichi in contemporanea; in tale ipotesi, infatti, tale soggetto, tendenzialmente, andrebbe a concentrarsi in misura maggiore sull'incarico principale, vale a dire quello per cui è stato assunto, piuttosto che sul differente incarico di DPO, specie se le mansioni svolte in via principale siano oggetto di valutazione, oppure se il loro adempimento possa determinare il riconoscimento di premialità. Sulla scorta di questa considerazione, l'EDPS ha sostenuto la necessità che il soggetto nominato quale DPO si occupi esclusivamente di detta funzione, e che, qualora le istituzioni più piccole non possano permettersi di nominarne uno per ciascuna, possa essere nominato un DPO per più unità.

Ma l'indipendenza è da intendersi anche come necessità che il DPO non venga condizionato da eventuali interferenze da parte di coloro che rivestono posizioni apicali nell'ambito delle istituzioni o organismi, i quali non possono contestare le determinazioni assunte dallo stesso; altresì, essa comporta la necessità che al DPO vengano garantite adeguate risorse economiche, informatiche e a livello di staff, che questi possa gestire autonomamente, e rispetto alle quali sarà tenuto a presentare il rendiconto solo al termine del proprio mandato.

Nel *paper*, inoltre, viene dato atto dell'esistenza di un *network* di *Data Protection Officers* i quali, incontrandosi regolarmente, al fine di scambiare punti di vista circa lo svolgimento e le problematiche derivanti dall'esercizio delle loro funzioni, potranno formulare pareri o consigli utili in tema di protezione dei dati per tutti i DPO, anche quelli non operanti esclusivamente nell'ambito delle istituzioni europee.

4.2 Il "*Professional Standards for Data Protection Officers of the EU Institution and Bodies Working under Regulation (EC) 45/2001*"

Quale primo risultato del lavoro del *network,* nell'ottobre del 2010, vedeva luce il documento "*Professional Standards for Data Protection Officers of the EU Institution and Bodies Working under Regulation (EC) 45/2001*"[278].

Il documento in questione è stato realizzato principalmente al fine di delineare gli standard minimi dello *status* di DPO, nonché al fine di venire in aiuto ai DPO operanti nelle realtà istituzionali europee, suggerendo agli stessi delle "*best practices*" cui attenersi nell'esercizio delle funzioni. Altresì, viene chiarito alle istituzioni ed organizzazioni europee che genere di impegno devono aspettarsi dal DPO nominato, e come possono valutarne la *performance*.

Il profilo più interessante del documento, tuttavia, è da rintracciarsi nella caratterizzazione del DPO che viene presentata. Dopo aver ribadito come il DPO rivesta un ruolo fondamentale nell'ambito dell'organigramma istituzionale, garantendo il rispetto, da parte degli enti, della disciplina in materia di protezione dei dati, viene specificato come gli obblighi derivanti da tale funzione vengano assolti non solo attraverso l'esercizio dei compiti tipici di consulenza nei confronti dei titolari del trattamento, ma anche attraverso una funzione di vigilanza e monitoraggio, svolti in maniera indipendente, sull'effettiva applicazione delle regole nell'ambito dell'istituzione o organismo[279].

Il documento prosegue poi con l'analisi dettagliata di tutto ciò che concerne la figura in questione: le caratteristiche professionali[280]e personali[281] che questi deve

---

[278] Tale documento è rinvenibile al link *http://ec.europa.eu/dataprotectionofficer/docs/dpo_standards_en.pdf*.

[279] Nel testo si legge "*the DPO plays a fundamental role in ensuring respect of data protection requirements within the institution/body. The DPO is appointed by his institution to advise it on the application of the rules, but he/she is also required to ensure, in an independent manner, that the Regulation is applied internally. The DPO's dual responsibility is reflected in particular in the cooperation he has to develop with the EDPS*".

[280] Professionalmente, il DPO deve avere i seguenti requisiti:

(a) *Expertise in the area of EU privacy and data protection law, in particular Article 16 of the Treaty on the Functioning of the European Union, Article 8 of the Charter of Fundamental Rights of the European Union, Regulation (EC) 45/2001 and other relevant data protection legal instruments, and expertise in IT and IT Security;*

(b) A good understanding of the way the institution operates and of its personal data processing activities, and an ability to interpret relevant data protection rules in that context.

[281] I requisiti di carattere personale sono tre:

(a) *It is recommended that the DPO should have the following experience/maturity: at least 3 years of relevant experience2 to serve as DPO in a body where data protection is not related to*

possedere per essere scelto all'atto della selezione; la necessità che gli venga garantita una formazione continua[282] e che gli vengano rilasciate le eventuali certificazioni[283]; i requisiti caratterizzanti il suo *status*, con particolare riferimento al carattere dell'indipendenza[284]; i doveri ed i poteri, i rapporti con gli altri organi dell'istituzione[285], i rapporti con i soggetti interessati[286], i rapporti con l'EDPS[287], ed infine gli standard etici.

---

the core business3 (and thus personal data processing activities are mainly administrative); and at least 7 years of relevant experience2 to serve as DPO in an EU institution or in those EU bodies where data protection is related to the core business or which have an important volume of processing operations on personal data.
(b) Personal skills: integrity, initiative, organization, perseverance, discretion, ability to assert himself/herself in difficult circumstances, interest in data protection and motivation to be a DPO.
(c) Interpersonal skills: communication, negotiation, conflict resolution, ability to build working relationships.

[282] La formazione in questione può essere realizzata attraverso corsi offerti dal Garante Europeo o dalle istituzioni e organismi europei, o anche da enti esterni; viene finanche fatto riferimento alla necessità che il DPO partecipi al *network* dei DPOs e studi i documenti offerti dal *network*, ritenendoli strumenti idonei a garantirne la formazione.

[283] A tal riguardo, il documento chiarisce che la certificazione più rilevante è quella rilasciata dall'IAPP (*International Association of Privacy Professionals*), che offre varie certificazioni in materia di *privacy*, incluse la CIPP (*Certified Information Privacy Professional*) e la CIPP/IT (*Certified Information Privacy Professional/Information Technology*).

[284] Per tali ragioni viene previsto che l'incarico abbia una durata compresa tra i due e i cinque anni, e che possa essere rinnovato fino ad un massimo di dieci anni; che il nominativo del DPO sia registrato presso l'EDPS; che il DPO possa essere rimosso dall'incarico esclusivamente se non è più in possesso delle condizioni richieste per l'esercizio delle sue funzioni, e che in tal caso si rende necessario il consenso del Garante europeo. Viene, altresì, previsto che allo stesso siano garantiti uno staff e le risorse necessarie, ed ancora che questi sia sollevato da altri incarichi eventualmente ricoperti nell'ambito dell'istituzione o organismo, allorquando si riscontrino conflitti di interesse tra le funzioni svolte.

[285] Il DPO deve garantire la formazione dei Titolari e del loro personale, formazione che mira ad individuare le misure pratiche da adottare per conformarsi ai requisiti di protezione dei dati. Tale formazione dovrebbe essere svolta in modo continuativo, sia al fine di garantire il costante aggiornamento del personale, sia per garantire che eventuali nuovi assunti siano adeguatamente istruiti in materia di protezione dei dati. Per i gruppi di personale che trattano in maniera diretta i dati dovrebbe poi essere previsto lo svolgimento di sessioni specifiche di formazione. Tra i compiti del DPO rientra anche quello di sviluppare, se del caso, insieme ai Titolari del trattamento, linee guida per la protezione dei dati, specie allorquando vi sia un numero considerevole di persone all'interno dell'organizzazione chiamato ad elaborare i dati personali. Ancora, il DPO deve partecipare alle riunioni della dirigenza o incontrare, almeno due volte l'anno, gli organi direttivi, al fine di essere aggiornato sullo stato di attuazione della normativa e sulla conformità alla stessa di ogni trattamento posto in essere da parte dell'organizzazione. Il DPO, inoltre, può creare una pagina Intranet per la protezione dei dati nell'istituzione/organo, che includa il Registro da questi tenuto, le dichiarazioni sulla *privacy* rilasciate dal Titolare, le linee guida e le istruzioni che l'istituzione/organo deve seguire, i pareri del Garante sui controlli preliminari dell'istituzione/organo, i rapporti periodici del DPO e qualsiasi altro elemento che possa essere utile al Titolare del trattamento e al personale alle sue dipendenze. Ancora, deve pubblicare brevi articoli e rapporti regolari in qualsiasi *newsletter* interna esistente, preparare brevi opuscoli informativi, cartelle etc. Se le dimensioni dell'istituzione lo giustificano, il DPO dovrebbe incoraggiare la creazione di una rete di corrispondenti/coordinatori DPO locali. È previsto, altresì, che le istituzioni possano adottare ulteriori regole che prevedano un rafforzamento dei poteri del DPO in campo "investigativo", nonché l'onere per gli stessi di cooperare con il DPO, ed ancora il

Non manca, nel *paper*, ed anzi è rilevante al punto da richiedere una più approfondita analisi, l'indicazione di una serie di circostanze concrete che potrebbero incidere e condizionare in negativo il corretto adempimento delle funzioni di DPO.

Aldilà dei problemi che potrebbero sorgere in virtù della carenza delle competenze personali adatte a svolgere il ruolo in questione, che potrebbero chiaramente avere un'influenza negativa determinante sull'esercizio delle funzioni (come nel caso in cui la persona nominata si riveli essere non sufficientemente in grado di gestire la mole di lavoro, oppure non in grado di fronteggiare determinate problematiche, o, ancora, di negoziare validamente in caso di problemi *etc.*), altre ipotesi possono essere rintracciate nel caso, già posto in evidenza dall'EDPS, in cui, ad esempio, il ruolo di DPO venga svolto *part-time*, in concomitanza con altro ruolo per il quale il soggetto è già titolare di un rapporto di lavoro alle dipendenze dell'istituzione/organismo: ricorrendo tale evenienza, è chiaro che il DPO dovrebbe calibrare i tempi e le risorse utili per svolgere diligentemente entrambe le funzioni, tuttavia è anche probabile che concentri le proprie energie nelle attività proprie della sua funzione "principale", perché interessato agli avanzamenti di carriera o, più in generale, alle valutazioni positive sulla *performance*.

---

diritto del DPO di avere sempre accesso agli uffici, ai locali, alle operazioni di trattamento dei dati, ai *server* in cui i dati sono conservati.

[286] Il DPO ha l'onere di assicurare che gli interessati siano informati dei loro diritti ai sensi del Regolamento (articolo 24, paragrafo 1, lettera a). Tali informazioni possono essere fornite attraverso una pagina *Internet*, e i requisiti che le stesse devono possedere sono stabiliti negli articoli 11 e 12 del Regolamento: sul DPO graverà l'obbligo di garantire che il Titolare abbia adottato tutte le misure necessarie per soddisfare detti requisiti, obbligo che può essere assolto dallo stesso attraverso l'assistenza ai Titolari nella redazione dei documenti informativi.

[287] Il DPO ha il dovere di cooperare con l'Autorità (art. 24 (1) (b)). Questi è responsabile nei confronti dell'EDPS, sia nel senso di dover rispondere alle richieste a lui indirizzate, sia nel senso di garantire che quelle indirizzate ai responsabili siano conosciute da questi ultimi. In generale, l'EDPS invia richieste al DPO per i seguenti scopi:

- integrare le informazioni fornite in una notifica per il controllo preventivo;
- avere informazioni in merito ad un reclamo riguardante l'istituzione o l'organismo di cui il DPO è dipendente;
- monitorare i progressi dell'istituzione nell'attuazione delle raccomandazioni dell'EDPS;
- raccogliere informazioni per un'indagine in corso relativa a qualche specifico problema.

Il DPO dovrebbe rispondere a tutte le richieste entro un termine ragionevole (normalmente, entro due settimane dal ricevimento della richiesta). Se è necessario più tempo, all'EDPS deve essere indicata la data entro la quale si provvederà a rispondere.

Ancora, un altro problema potrebbe sorgere nel caso in cui l'incarico venga assegnato ad un dipendente con contratto a tempo determinato, per lo svolgimento di funzioni distinte da quelle di DPO, ma assegnate in concomitanza: questi si troverebbe maggiormente esposto a situazioni di conflitto, ed in una posizione più debole rispetto al lavoratore a tempo indeterminato, in quanto tenderebbe a concentrarsi di più sulle funzioni proprie dell'incarico per cui è stato assunto, al fine di ottenere, eventualmente, un rinnovo del contratto. Stessa circostanza si verificherebbe nell'ipotesi in cui venga nominato DPO un lavoratore alle dipendenze delle istituzioni/organismi da breve tempo, considerato che questi, quasi certamente, avrà maggiore interesse a sviluppare le competenze necessarie per quella che potrebbe considerare l'attività principale. Peraltro, non appare da escludere, che, proprio in ipotesi di questo tipo, il dipendente potrebbe avere qualche difficoltà nei rapporti con i superiori (gerarchici). In relazione a quest'ultimo punto, tuttavia, nel documento viene fatto presente che è il ruolo del DPO, comunque inteso, a poter creare delle difficoltà per qualsiasi soggetto già dipendente dell'organismo che cumuli un doppio ruolo: una puntuale e precisa esecuzione dei compiti di DPO, infatti, richiede spesso che l'incaricato mantenga un atteggiamento fermo, a volte duro, anche con i superiori gerarchici. Ovviamente, ciò può determinare delle forti pressioni, ed è per questo che diventa necessario garantire al DPO la possibilità di riferire esclusivamente al responsabile amministrativo dell'istituzioni o dell'ente, soprattutto per i dipendenti part-time, i quali dovrebbero riferire direttamente all'autorità che ha li ha nominati, e da questa essere "controllati".

Ancora, potrebbe minare il requisito dell'indipendenza anche la necessità, per il DPO, di dover richiedere al proprio superiore la messa a disposizione delle risorse necessarie per l'esercizio di tale funzione, risorse che comprendono sia utilità economiche, sia unità di personale alle quali demandare determinati adempimenti. In tal caso, la difficoltà potrebbe consistere nella mancata attivazione da parte del capo ufficio, considerato che questi potrebbe non essere del tutto interessato a dimostrarsi *compliant* in materia di protezione dei dati: tale circostanza, secondo il *network*, potrebbe essere superata attraverso la predisposizione *ab initio* di un *budget*, della cui gestione diverrebbe responsabile il DPO in via esclusiva, con la

possibilità di richiedere un'autorizzazione al superiore gerarchico in caso di necessità di eventuali risorse aggiuntive.

In considerazione delle problematiche esposte, il *network* di DPOs ha individuato alcune *best practices* che possono essere adottate dalle istituzioni, tra le quali, ad esempio, quella di nominare quale DPO un soggetto che rivesta un ruolo apicale nell'organigramma dell'istituzione, per un periodo di tempo sufficientemente lungo (anche, ad esempio, cinque anni), e, possibilmente, un soggetto che abbia stipulato con l'istituzione un contratto a tempo indeterminato già da un congruo lasso di tempo. Viene suggerito, inoltre, di nominare una persona che possa dedicarsi completamente allo svolgimento di tale ruolo, soprattutto nelle istituzioni di grandi dimensioni[288], ma anche in quelle più piccole, per lo meno nella fase iniziale di costituzione di un regime di protezione dei dati.

Qualora, invece, si scegliesse di conferire il ruolo di DPO ad un soggetto che si occupi già di altre funzioni, è necessario che queste non diano adito ad un possibile conflitto di interessi, quindi sarà importante valutare con attenzione quale soggetto incaricare. Inoltre, è necessario tutelare quest'ultimo, poiché egli non dovrà subire alcun pregiudizio a causa dell'esercizio delle funzioni di DPO, soprattutto con riferimento a possibili avanzamenti di carriera: a tal fine, viene suggerito di valutare, ai fini della *performance*, non solo le funzioni relative all'incarico originario, ma anche quelle relative all'incarico di DPO, ed altresì – qualora previsto dalle norme dell'istituzione/organismo- viene suggerito che l'EDPS abbia l'opportunità di esprimere anch'esso un parere sulla *performance* dell'attività svolta in qualità di DPO.

Infine, viene evidenziata la necessità di predisporre, all'interno dell'organizzazione, delle regole che garantiscano l'obbligo da parte di tutto il personale di collaborare con il DPO senza che per ciò sia necessario un ordine ovvero un'autorizzazione preventiva da parte del superiore gerarchico.

[288] In particolare, nelle istituzioni la cui attività principale consiste nel trattamento di dati personali, è necessario che i DPO non solo svolgano in via esclusiva il ruolo, ma che gli stessi possano avvalersi di un vero e proprio staff a loro completo servizio.

5. Il *Data Protection Officer* in Germania

Sebbene, come si è visto, il legislatore europeo non fosse nuovo alla considerazione di una figura professionale di DPO, prima di procedere all'analisi delle disposizioni del GDPR, è interessante rivolgere l'attenzione alla disciplina dello Stato membro che ha ispirato, più di ogni altro, il legislatore europeo nella formulazione della nuova disciplina, cioè l'ordinamento tedesco, sebbene, come già accennato, in vari altri ordinamenti vi fosse già traccia di questa figura o di figure similari[289].

L'introduzione della figura del *datenschtzbeauftrager* (DSB), considerata l'antesignana del DPO nella legislazione tedesca, ha radici lontane dal momento che in Germania, la prima normativa in materia di protezione dei dati personali, a livello federale, fu emanata il 27 gennaio 1977 (*Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung)*. Successivamente la normativa federale in tema di tutela dei dati personali *Bundesdatenschutzgesetz (BDSG)* è stata modificata, novellata ed integrata una prima volta nel 1990 (BDSG 1990)[290], e successivamente nel 2001 (BDSG 2001), nel 2003 (BDSG 2003, adeguata ai principi della Direttiva 95/46/CE), nel 2007 (BDSG 2007), nel 2010 (BDSG 2010), fino all'ultima modifica avvenuta nel 2017 (BDSG 2017)[291].

La disciplina dettata dal legislatore tedesco in materia di protezione dei dati personali manifesta in maniera evidente una radicata convinzione circa la capacità delle aziende di essere in grado di conformare, in maniera proattiva, il proprio comportamento alle norme di legge al fine di prevenire qualsiasi evento dannoso[292]. Non è un caso che il legislatore abbia deciso di incentrare il sistema di protezione dei dati personali - che gli studiosi hanno ribattezzato "modello consultivo" - sul principio dell'autocontrollo aziendale (o *self-liability*), che si

---

[289] In Francia, ad esempio, la legge 6 agosto 2004, che ha modificato la legge n. 78-17 del 3 gennaio 1978, recependo la Direttiva 95/46/CE, aveva già introdotto la figura facoltativa del *Correspondant à la protection des données à caractère personnel* (anche noto come CIL, *Correspondant informatique et libertés*). In Spagna, invece, era stata prevista, con il Real Decreto 1720/2007, la designazione di un *Responsable de securidad* nel *documento de seguridad* per l'ipotesi di trattamento di dati cui applicare misure di sicurezza di medio o alto livello.

[290] Legge 1990 BGBI.I.S.2954.

[291] Sull'evoluzione della disciplina del trattamento dei dati nel diritto tedesco, v. A ROBNAGEL (a cura di), *Handbuch Datenschutzrech. Die neuen Grundlagen für Wirtschaft und Verwaltung*, Munich, 2003.

[292] Cfr. F. BIGNAMI, *Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy*, 59 AM. J. COMP. L. 411, 424–30 (2011).

esplica nell'imposizione di specifici obblighi in capo al titolare del trattamento, tra i quali rientra, appunto, la nomina obbligatoria di un funzionario interno per la *privacy* (*Beauftragter fur den Datenschutz - DSB*).

Il legislatore tedesco aveva previsto, all'art. 36 della BDSG, che il "responsabile della protezione dei dati personali" (DSB) venisse nominato obbligatoriamente da ogni entità pubblica e da ogni soggetto privato che si occupi regolarmente del trattamento automatizzato di dati personali[293] e che occupasse dieci dipendenti a tempo indeterminato a tale scopo[294], prevedendo altresì che la nomina dovesse essere disposta entro un mese dall'inizio delle attività di trattamento. Il DSB, come soggetto responsabile della protezione dei dati, opera quale funzionario indipendente del titolare, riferendo esclusivamente al consiglio di amministrazione o all'amministratore delegato, e deve avere cognizione e cura degli aspetti, anche i più problematici, dei trattamenti posti in essere. Il secondo comma dell'art. 36 richiede, a tal fine, il necessario possesso di una conoscenza specialistica in materia di protezione dei dati, indicando le caratteristiche di affidabilità che il DSB deve possedere rispetto al tipo di trattamento posto in essere. Il legislatore tedesco, in ogni caso, non prevedeva che il DSB dovesse comprovare tale conoscenza specialistica attraverso una qualche particolare forma di certificazione: in ragione di questa circostanza, risultava molto problematico individuare il candidato ideale, specie per le aziende private, e soprattutto nel caso in cui ad essere nominato fosse un soggetto già dipendente dell'ente. Una volta nominato, era previsto che il mandato avesse una durata di 12 mesi, rinnovabili, e la risoluzione dell'incarico potesse avvenire esclusivamente per "gravi ragioni", vale a dire per gravi violazioni dei doveri contrattuali, od anche su proposta dell'Autorità di controllo.

In particolare, rispetto al GDPR, il modello tedesco individuava una articolata disciplina circa le ipotesi, le condizioni e i modi per la revoca dell'incarico,

[293] Il significato di "elaborazione automatizzata" è stato ampiamente interpretato dalle Autorità tedesche: allo stato attuale, con tale definizione, si vuol fare riferimento ad ogni dipendente che tratti i dati personali mediante un computer aziendale.

[294] La nomina era altresì prevista come obbligatoria nel caso di trattamenti non automatizzati, per i quali fossero impiegai almeno 20 dipendenti. Inoltre, indipendentemente dal numero di persone occupate ai fini dell'elaborazione dei dati, tutti gli enti privati erano tenuti a nominare un DPO nel caso di trattamenti di dati a fini commerciali, a fini di attività di profilazione, per ricerche di mercato, ovvero nel caso di trattamenti di dati sensibili.

garantendo una tutela particolarmente incisiva al DSB: basti soltanto considerare che, in caso di conflitto con il consiglio di amministrazione o con l'amministratore delegato, il DSB avrebbe potuto chiedere il sostegno dell'Autorità di controllo; ed ancora si consideri che la nomina poteva essere revocata solo previo parere dell'Autorità, salvo le ipotesi di licenziamento per giusta causa[295].

Ai sensi dell'art. 37, sul DSB grava l'obbligo di garantire che le disposizioni della *Bundesdatenschutzgesetz* e delle altre normative in materia di protezione dei dati personali siano rispettate dall'ente presso il quale è stato nominato, sebbene, in ogni caso, gravi esclusivamente sul titolare del trattamento la responsabilità verso terzi per ogni decisione adottata e metodologia utilizzata in merito alla protezione dei dati personali.

Il numero di adempimenti gravanti sul DSB, che hanno riflesso sull'attività del titolare, è abbastanza cospicuo: questi possono comprendere, ad esempio, l'identificazione di eventuali *deficit* che rendono il trattamento non conforme alla disciplina normativa; la proposta di miglioramenti; il monitoraggio (anche attraverso un controllo preventivo) delle attività di trattamento; la consultazione; la tenuta di un registro pubblico delle attività di trattamento dei dati; le notifiche all'Autorità di controllo; la formazione del personale e la gestione dei reclami. Per poter ottemperare compiutamente a tali compiti, è previsto che il DSB possa consultare in qualsiasi momento l'Autorità.

Ancora, il DSB deve essere informato tempestivamente sui progetti di elaborazione dei dati personali[296], ed è al contempo tenuto a controllare che i programmi per il trattamento dei dati siano utilizzati in maniera corretta da parte

---

[295] L'art. 626 BGB, rubricato "Licenziamento per giusta causa" recita: "*Il rapporto di lavoro può essere risolto da una delle parti del contratto per giusta causa senza preavviso, se ci sono fatti in base ai quali la parte che recede, tenendo conto di tutte le circostanze di ciascun caso e ponderando gli interessi di entrambe le parti, continuare il rapporto di lavoro fino alla scadenza del periodo di preavviso o fino alla risoluzione consensuale del rapporto di lavoro non può essere previsto. La comunicazione può essere presentata entro due settimane. Il periodo decorre dalla data in cui la persona legittimata alla cessazione viene a conoscenza dei fatti rilevanti. La parte deve notificare all'altra parte, su richiesta scritta e senza ritardi la ragione del licenziamento*".

[296] Tra le informazioni che il Titolare deve rilasciare rientrano, ai sensi dell'art. 37 c. 2, quelle relative ai sistemi di elaborazione utilizzati per il trattamento, alla denominazione ed ai tipi di file contenenti i dati, alla tipologia dei dati memorizzati, ai motivi per cui si è resa necessaria la conoscenza di tali dati, ai destinatari cui i dati possono essere comunicati, all'indicazione dei soggetti autorizzati a prenderne visione.

degli incaricati. Per tali ragioni, dovrà individuare le modalità idonee a rendere gli incaricati costantemente aggiornati rispetto alla disciplina normativa, assistendo altresì il titolare in merito alla scelta di coloro i quali devono essere assegnati al trattamento. In tal senso, il DSB svolge un ruolo particolarmente incisivo anche con riferimento all'organigramma aziendale, potendo indirizzare l'azienda o l'ente verso la nomina dei soggetti ritenuti idonei e capaci a svolgere l'incarico.

Naturalmente, l'azienda che ha nominato il DSB sarà tenuta a fornire a questi ogni attrezzatura e risorsa necessaria per lo svolgimento delle sue funzioni.

Come clausola di chiusura della disciplina in esame, la legge prevedeva che le società potessero essere multate con importi fino a 50.000 euro per aver omesso, intenzionalmente o per negligenza, di nominare un DSB, ovvero per aver nominato una persona non qualificata, o, ancora, per non avergli fornito risorse adeguate per lo svolgimento dell'incarico.

Il portato applicativo della disciplina in tema di DSB ha portato indubbiamente esiti postivi, sia in termini di implementazione della *compliance* aziendale, sia in termini di garanzia per i diritti degli interessati, ponendosi, appunto, come modello per il legislatore del GDPR, come peraltro emerge anche dalla considerazione delle Linee Guida adottate il 13 dicembre 2016 dal WP29[297].

6. La disciplina normativa del *Data Protection Officer* nel GDPR

Il GDPR dedica tre norme alla figura ed al ruolo del DPO (artt. 37, 38, e 39), che si occupano, rispettivamente della "designazione", della "posizione", e dei "compiti".

Deve sottolinearsi, in un'ottica di sistema, come la prima ed immediata novità del GDPR, correlata all'introduzione del DPO, consiste nell'aver eliminato l'obbligo del titolare di notificare previamente i trattamenti posti in essere all'Autorità di controllo (obbligo che, come si è evidenziato, era previsto dall'art. 18 della Direttiva 95/46/CE[298]).

[297] Cfr. "*Linee guida sui responsabili della protezione dei dati (RPD) adottate dal Gruppo Art. 29 il 13 dicembre 2016 ed emendate il 5 aprile 2017 (WP243 rev. 01)"* reperibili al link https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.

[298] È bene rilevare che il Regolamento prevede in ogni caso che gli Stati membri possano introdurre eventualmente la previsione di un obbligo di notificazione per attività specifiche (ad esempio per i trattamenti di dati relativi a procedimenti penali).

Tale modifica, espressione evidente del passaggio "da una valutazione generale e accentrata presso l'autorità di controllo" ad una valutazione "decentrata e affidata *in primis* ai titolari del trattamento"[299] si spiega proprio in considerazione dell'introduzione della complessa serie di obblighi gravanti sul titolare del trattamento, cui si è fatto riferimento più volte[300], che renderebbero superfluo aggravare la sua attività con la previsione di un ulteriore adempimento che, peraltro, si era rivelato in passato essere ben poco efficace[301]. Tra questi obblighi spicca, con ogni evidenza, quello di nomina del DPO, figura professionale che viene istituzionalizzata in ogni realtà pubblica o privata, con l'eccezione, in riferimento al settore privato, delle piccole imprese e delle microimprese; queste ultime, proprio in ragione del ridotto volume di dati che può essere interessato dal giro di affari e che non dovrebbe presentare significativi indici di rischio, non saranno tenute ad avvalersi di un DPO (obbligo che invece potrebbe rivivere in ipotesi di trattamenti con indice di rischio elevato). Sembra potersi rintracciare, anche in tal caso, una somiglianza col regime normativo di cui all'art. 18 della Direttiva n.95/46/CE, ove era stabilito che l'obbligo di notifica poteva venir meno, in alternativa alla nomina del *Data protection official*, nel caso in cui il titolare avesse posto in essere trattamenti non rischiosi di dati personali.

Alla luce di quanto sopra, è facile notare il cambio di paradigma che ha interessato la disciplina: ciò che prima costituiva una mera eccezione alla regola, diviene ora una regola operativa, che coinvolge tutti i soggetti pubblici e la stragrande maggioranza dei soggetti privati. Ed il mutamento non è solo di natura formale,

---

[299] R. TORINO, op. cit., p. 857.

[300] Tra gli obblighi, non può non farsi riferimento in questa sede, alla luce del citato venir meno dell'obbligo di notificazione, a quello, sancito dall'art. 30 GDPR, avente ad oggetto la predisposizione, ad opera del titolare, di un registro che indichi, in maniera esaustiva, tutte le attività di trattamento svolte: tale registro potrà poi essere fornito alle Autorità di controllo, su richiesta, in qualsiasi momento e potrà essere altresì consultato in qualsiasi momento dagli interessati del trattamento. Si tratta di un registro che va sostanzialmente a sostituire quello che prima era tenuto dall'Autorità, ove venivano iscritti tutti i trattamenti segnalati dai titolari.

[301] Nel considerando n. 70 dei lavori preparatori del Regolamento si legge che "*La direttiva 95/46/CE ha introdotto un obbligo generale di notificare alle autorità di controllo il trattamento dei dati personali. È pertanto necessario abolire tale obbligo generale e indiscriminato di notificazione e sostituirlo con meccanismi e procedure efficaci che si concentrano piuttosto su quelle operazioni di trattamento che potenzialmente presentano rischi specifici per i diritti e le libertà degli interessati, per la loro natura, portata o finalità. in tali casi, è opportuno che il responsabile del trattamento o l'incaricato del trattamento effettui una valutazione di impatto sulla protezione dei dati prima del trattamento, che verte in particolare anche sulle misure, sulle garanzie, sui meccanismi previsti per assicurare la protezione dei dati personali e il rispetto del presente Regolamento*".

ma piuttosto sostanziale: se, infatti, il controllo preventivo dell'Autorità si rivelava, in passato, spesso privo di incisività, dovendo la stessa passare in rassegna ogni trattamento notificatole e dunque non potendo concentrarsi solo su quelli effettivamente rischiosi (salvo i trattamenti notificati ai sensi dell'art. 20), adesso il controllo sulle attività è ancora più incisivo, in quanto affidato ad un soggetto specializzato, chiamato ad operare in una realtà caratterizzata dall'interesse del titolare ad essere *accountable*, conformandosi alle indicazioni e pareri del DPO, fatta in ogni caso salva la possibilità per l'Autorità pubblica di intervenire in particolari casi.

Tuttavia, come si avrà modo di vedere, potrebbe esservi la possibilità che si verifichino delle criticità, stante la generalità e astrattezza della disciplina della figura del DPO, che in certi punti si presta ad essere criticata proprio in ragione della sua genericità e astrattezza.

6.1 La nomina del *Data Protection Officer*

Ai sensi dell'art. 37 GDPR, il DPO deve essere designato dal titolare del trattamento, e dal responsabile del trattamento, ogni qualvolta:

- il trattamento sia effettuato da un'autorità pubblica o da un organismo pubblico, eccetto le autorità giurisdizionali nell'esercizio delle loro funzioni[302];
- le attività principali del titolare o del responsabile consistano in trattamenti che comportino il monitoraggio regolare e sistematico degli interessati su larga scala;
- le attività principali del titolare o del responsabile consistano nel trattamento, su larga scala, di categorie particolari di dati personali ex art. 9[303] e di dati relativi a condanne penali o reati ex art. 10.

[302] Il D. Lgs. 10 agosto 2018, n. 101, recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679, che ha novellato estensivamente il Codice della protezione dei dati personali (D. Lgs. 196/2003), ha tuttavia introdotto, all'art. 2-*sexiesdecies*, rubricato "Responsabile della protezione dati per i trattamenti effettuati dalle autorità giudiziarie nell'esercizio delle loro funzioni", l'obbligo di nomina del DPO anche per le autorità giudiziarie nell'esercizio delle loro funzioni. Nell'articolo in questione, infatti, non viene utilizzata la formula "possono designare", bensì "designano".

[303] Ai sensi dell'art. 9 i dati rientranti in tali categorie sono i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Il legislatore europeo, nel fare riferimento ai soggetti pubblici, non offre una definizione degli stessi, ma rinvia al diritto domestico dello Stato di appartenenza. La mancanza di una definizione legislativa, o meglio, il rinvio alle singole legislazioni, rischia di lasciare pericolosamente il concetto di "soggetto pubblico" in una dimensione nebulosa, con ciò che può conseguirne, in punto di responsabilità dei soggetti in questione, data l'incertezza sull'obbligatorietà o meno per essi della designazione del DPO. Per tali ragioni, la dottrina si è interrogata circa le modalità attraverso le quali individuare i soggetti in questione in ambito nazionale, ed in particolare se, ai fini di tale individuazione, concorra la natura giuridica dell'ente o dell'organismo considerato, ovvero la natura delle attività svolta, e dunque debba seguirsi un parametro di tipo funzionale.

Il WP29 ha avuto cura di precisare che, se certamente sono da considerarsi «autorità pubbliche o organismi pubblici le autorità nazionali, regionali e locali […] a seconda del diritto nazionale applicabile, la nozione (potrebbe) ricomprende(re) anche tutta una serie di altri organismi di diritto pubblico»[304]. A titolo esemplificativo, il WP29 richiama inoltre i concetti di "ente pubblico" e di "organismo di diritto pubblico" di cui all'art. 2, paragrafi 1 e 2, della direttiva 2003/98/CE, relativa al riutilizzo dell'informazione del settore pubblico. Ai sensi di tale disciplina, per "ente pubblico" devono intendersi «le autorità statali, regionali o locali, gli organismi di diritto pubblico e le associazioni formate da una o più di tali autorità oppure da uno o più di tali organismi di diritto pubblico»; mentre rientrano nella nozione di "organismi di diritto pubblico" gli enti istituiti per soddisfare specificatamente bisogni d'interesse generale aventi carattere non industriale o commerciale, quanto meno in via prevalente, che siano dotati di personalità giuridica e che presentino, inoltre, almeno uno dei seguenti tratti sintomatici: il finanziamento dell'attività, la soggezione al controllo di gestione, oppure la designazione di più della metà dei componenti degli organi di amministrazione, di direzione o di vigilanza da parte dello Stato, di enti pubblici territoriali o di altri organismi di diritto pubblico.

[304] Cfr. "*Linee guida sui responsabili della protezione dei dati (RPD) adottate dal Gruppo Art. 29 il 13 dicembre 2016 ed emendate il 5 aprile 2017 (WP243 rev. 01)"*, par. 2.1.1., p. 6., nota n. 12, rinvenibile al link *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048*.

Tuttavia, il richiamo a tale normativa non aiuta l'interprete, in primo luogo perché manca nel GDPR un rinvio generale alla direttiva 2003/98/CE, ed in secondo luogo poiché non appare possibile ricorrere ad un'interpretazione conforme o analogica rispetto alla disciplina dettata da quest'ultima[305].

In considerazione della mancanza di una specifica definizione a livello europeo, occorre dunque fare riferimento al diritto nazionale. Com'è noto, però, in Italia manca una nozione unitaria e formale di "soggetto pubblico", essendo al contrario la stessa "frammentaria e sostanziale", tant'è che l'ambito soggettivo di applicazione di ogni disciplina di settore deve essere perimetrato sulla base non tanto della natura giuridica del soggetto considerato, ma della funzione perseguita dallo stesso[306]. Perciò, analizzando la normativa esistente, si dovrebbe fare riferimento all'art. 1 c. 2 del D. Lgs. 165/2001 (Testo Unico del Pubblico Impiego)[307], sebbene possano venire in rilievo anche le definizioni dettate rispettivamente dall'art. 2, c. 2 del D. Lgs. 82/2005 (Codice dell'Amministrazione digitale)[308], e dall'art. 2 bis del D. Lgs. 33/2013 (c.d. "Decreto trasparenza")[309]. In

---

[305] Come evidenziato già da attenta dottrina, va esclusa sia un'interpretazione di tipo conforme che di tipo analogico, "*la prima in quanto non vi è una gerarchia tra le due normative, non potendosi ritenere che la direttiva sul riutilizzo dei dati sia preminente rispetto al GDPR, di modo che viene a mancare il presupposto che legittimerebbe una interpretazione conforme di questo rispetto a quella. La seconda, invece, poiché la ratio delle due discipline è differente, e pertanto non possono applicarsi analogicamente le norme dell'una alle fattispecie non regolate dall'altra. Infatti, mentre la direttiva 2003/98/CE ha come obiettivo lo sfruttamento economico dei dati in possesso delle amministrazioni statali, attraverso il riutilizzo di essi, il GDPR, pur incentivando la libera circolazione delle informazioni, persegue il primario scopo della protezione dei dati delle persone fisiche: nulla, dunque, che giustifichi un'estensione in via interpretativa delle stesse norme*". V. N. MINISCALCO, *DPO obbligatorio per i soggetti pubblici, ma non per tutti: il problema*, rinvenibile al *link https://www.agendadigitale.eu/sicurezza/dpo-obbligatorio-per-i-soggetti-pubblici-ma-non-per-tutti-il-problema/*.

[306] *Ibidem*.

[307] Ai sensi dell'art. 1, c. 2 del D. Lgs. 30 marzo 2001, n. 165 "*per amministrazioni pubbliche si intendono tutte le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le Comunità montane, e loro consorzi e associazioni, le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio, industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti i del Servizio sanitario nazionale, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN) e le Agenzie di cui al decreto legislativo 30 luglio 1999, n. 300. Fino alla revisione organica della disciplina di settore, le disposizioni di cui al presente decreto continuano ad applicarsi anche al CONI*".

[308] Ai sensi dell'art. 2, c. 2 del D. Lgs. 7 marzo 2005, n. 82, le disposizioni della disciplina si applicano

"*a) alle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione, ivi comprese le partorita di sistema portuale, nonché alle autorità amministrative indipendenti di garanzia, vigilanza e regolazione;*

considerazione della vasta elencazione contenuta in tali norme, è evidente la difficoltà di individuare in concreto quali enti siano effettivamente investiti dell'obbligo di nomina del DPO.

Il Garante Privacy italiano, sulla scorta del parere già reso dal WP29, ha avuto cura di specificare che i soggetti in questione sarebbero quelli indicati dagli articoli 18-22 del Codice Privacy, ove sono altresì contenute le regole generali per i trattamenti da questi effettuati[310]. Rientrerebbero dunque in tale disposizione le amministrazioni dello Stato, anche con ordinamento autonomo, gli enti pubblici non economici nazionali, regionali e locali; le Regioni e gli enti locali; le università; le Camere di commercio, industria, artigianato e agricoltura; alle aziende del Servizio sanitario nazionale; le Autorità indipendenti. Il Garante ha inoltre precisato che «nel caso in cui soggetti privati esercitino funzioni pubbliche (in qualità, ad esempio, di concessionari di servizi pubblici), può risultare

---

b) ai gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse;
c) alle società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175, escluse le società quotate di cui all'articolo 2, comma 1, lettera p), del medesimo decreto che non rientrino nella categoria di cui alla lettera b)".

[309] Ai sensi dell'art. 2 bis del D. Lgs. 14 marzo 2013, n. 33 "*per "pubbliche amministrazioni" si intendono tutte le amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni, ivi comprese le autorità portuali, nonché le autorità amministrative indipendenti di garanzia, vigilanza e regolazione. La medesima disciplina prevista per le pubbliche amministrazioni di cui al comma 1 si applica anche, in quanto compatibile:*
a) agli enti pubblici economici e agli ordini professionali;
b) alle società in controllo pubblico come definite dall'articolo 2, comma 1, lettera m), del decreto legislativo 19 agosto 2016, n. 175. Sono escluse le società quotate come definite dall'articolo 2, comma 1, lettera p), dello stesso decreto legislativo, nonché le società da esse partecipate, salvo che queste ultime siano, non per il tramite di società quotate, controllate o partecipate da amministrazioni pubbliche;(lettera così sostituita dall'art. 27, comma 2-ter, d.lgs. n. 175 del 2016, introdotto dall'art. 27 del d.lgs. n. 100 del 2017)
c) alle associazioni, alle fondazioni e agli enti di diritto privato comunque denominati, anche privi di personalità giuridica, con bilancio superiore a cinquecentomila euro, la cui attività sia finanziata in modo maggioritario per almeno due esercizi finanziari consecutivi nell'ultimo triennio da pubbliche amministrazioni e in cui la totalità dei titolari o dei componenti dell'organo d'amministrazione o di indirizzo sia designata da pubbliche amministrazioni.
La medesima disciplina prevista per le pubbliche amministrazioni di cui al comma 1 si applica, in quanto compatibile, limitatamente ai dati e ai documenti inerenti all'attività di pubblico interesse disciplinata dal diritto nazionale o dell'Unione europea, alle società in partecipazione pubblica come definite dal decreto legislativo emanato in attuazione dell'articolo 18 della legge 7 agosto 2015, n. 124, e alle associazioni, alle fondazioni e agli enti di diritto privato, anche privi di personalità giuridica, con bilancio superiore a cinquecentomila euro, che esercitano funzioni amministrative, attività di produzione di beni e servizi a favore delle amministrazioni pubbliche o di gestione di servizi pubblici".

[310] "*Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico*" rinvenibile al link *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7322110#1.*

comunque fortemente raccomandato, ancorché non obbligatorio, procedere alla designazione di un RPD»[311].

Con riferimento ai soggetti privati, invece, si può immediatamente rilevare come, contrariamente a quanto previsto nell'ordinamento tedesco, nel GDPR non vi è alcuna distinzione tra obbligo di designazione del DPO in virtù del criterio discretivo basato sull'elaborazione automatica o meno dei dati personali, combinato con quello basato sul carattere dimensionale dell'azienda, sebbene in un primo momento, nella proposta originaria della Commissione europea, fosse stato previsto l'obbligo di nomina solo per le aziende che impiegavano più di 250 dipendenti[312].

Il superamento dell'idea iniziale, che legava la nomina al limite dimensionale della realtà aziendale, si spiega anche in considerazione del principio di *risk-based approach* che permea l'intera normativa, spiegando i suoi effetti anche con riferimento alla nomina del DPO e richiedendo, appunto, che la valutazione circa l'obbligatorietà della nomina non sia legata ad un piano meramente strutturale – soggettivo e astratto - ma piuttosto ad un piano sostanziale – oggettivo e concreto – che tenga conto della natura e della rischiosità dello specifico trattamento[313].

Il legislatore europeo, anche a tal fine, ha deciso di optare per il ricorso al concetto di "larga scala", come criterio discretivo per la nomina obbligatoria o meno di un DPO da parte delle imprese private. Il titolare, infatti, sarà tenuto alla nomina del

---

[311] Ci si è interrogati, in particolar modo, su quale fosse il destino delle c.d. società *in house*, vale a dire i soggetti giuridici formalmente di diritto privato, il cui capitale è detenuto, parzialmente o interamente, da soggetti pubblici, nonché i soggetti di diritto privato che, sulla base di una concessione, svolgono funzioni pubbliche o esercitano un potere pubblico. L'indirizzo dottrinario prevalente sembra ammettere la possibilità di far rientrare tali soggetti entro la categoria degli organismi pubblici deputati a nominare il DPO. Cfr. A. AVITABILE, *Il data protection officer*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo*, op. cit., pp. 337-338.

[312] V. art. 25.2 della "*Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*". La Proposta prevedeva che la nomina del DPO fosse obbligatoria, oltre che nelle ipotesi in cui il trattamento fosse effettuato da un'autorità pubblica, anche nei casi di trattamenti effettuati da imprese con 250 dipendenti o più, e nei casi in cui le attività principali del Titolare o del Responsabile del trattamento consistessero in trattamenti richiedenti per loro natura, oggetto o finalità un controllo regolare e sistematico degli interessati.

[313] C. SOLINAS, op. cit., p. 893. L'A. prosegue "*sono le funzioni stesse del DPO (l'essere strumento di ausilio del Titolare o del Responsabile nell'organizzazione e nello svolgimento di un trattamento conforme alla normativa in materia, nonché l'essere egli stesso una misura di garanzia del corretto trattamento) a richiedere che l'obbligo, e finanche l'opportunità di nomina di un tale professionista, siano valutati in relazione all'attività di trattamento da svolgere e non alla mera dimensione del soggetto chiamato a svolgerlo*".

DPO nei casi in cui la sua attività abbia ad oggetto un trattamento che per sua natura richieda il monitoraggio regolare e sistematico di dati personali su larga scala[314], ovvero quando le attività principali consistano nel trattamento, sempre su larga scala, di categorie particolari di dati personali e di dati giudiziari.

Diventa, pertanto, necessario tracciare il perimetro della definizione di "larga scala", stante l'inesistenza di precisazioni normative circa il numero di trattamenti di dati personali che ne possano integrare il significato[315]. Potrebbe essere utile a tal riguardo richiamare il considerando 91, il quale, sebbene nel diverso ambito della valutazione d'impatto, fornisce una definizione di "trattamento su larga scala", indicando come tale quello che mira al trattamento di una notevole quantità di dati, e che potrebbe incidere su un vasto numero di interessati. Non si tratta, a ben vedere, di una definizione esaustiva, in quanto sarebbe altresì utile, se non necessario, chiarire il concetto di "notevole quantità di dati" e quello di "vasto numero di interessati", stante l'importanza per l'interprete di fare i conti con quantità precise, non potendosi lo stesso accontentare di enunciazioni teoriche[316].

---

[314] Nelle Linee Guida, il WP29 ha precisato, con riferimento al concetto di "attività principale" che occorre tenere presente il legame intercorrente tra il "*core business*" aziendale e l'attività di trattamento dei dati personali. A titolo esemplificativo, anche se l'attività principale di un ospedale non è il trattamento dei dati ma la salute dei pazienti, essendo le due attività strettamente collegate, l'attività di trattamento dei dati rientrerà nell'alveo delle attività principali, per cui un ospedale sarà tenuto a nominare un DPO. Situazione analoga è quella di una società di vigilanza, ove l'attività di sorveglianza è indissolubilmente legata all'attività di trattamento dei dati personali. Al contrario, se il trattamento dei dati è solo di supporto al "*core business*" (ad esempio vengono trattati i dati dei propri dipendenti per procedere ai pagamenti), le imprese non avranno l'obbligo di nomina del DPO. Per quanto attiene, invece, la nozione di "*monitoraggio regolare e sistematico*", la stessa non trova una definizione nel GDPR, ma, secondo le Linee guida del WP29, l'aggettivo "regolare" può avere almeno uno dei seguenti significati:

- che avviene in modo continuativo ovvero a intervalli definiti per un arco di tempo definito;
- ricorrente o ripetuto a intervalli costanti;
- che avviene in modo costante o a intervalli periodici.

L'aggettivo "sistematico", a sua volta, ha almeno uno dei seguenti significati:

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia.

Cfr. *Linee guida sui responsabili della protezione dei dati (RPD) adottate dal Gruppo Art. 29 il 13 dicembre 2016 ed emendate il 5 aprile 2017 (WP243 rev. 01)*.

[315] Inutile sottolineare che forse sarebbe stato preferibile quantificare un numero minimo di trattamenti svolti dal titolare (500/1000/2000 annui) al ricorrere del quale questi incorrerebbe nell'obbligo di nomina.

[316] G.B. GALLUS – M. PINTUS, *Data protection impact assessment*, in G. CASSANO - V. COLAROCCO, G.B. GALLUS, F.P. MICOZZI (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, Giuffrè, 2018, p. 181.

p. 181.

Il WP29, nelle Linee guida, ha suggerito di tenere in considerazione, al fine della definizione di concetto di "larga scala", i seguenti elementi: il numero dei soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; la durata, ovvero la persistenza, dell'attività di trattamento e, infine, la portata geografica dell'attività di trattamento[317].

Per quanto riguarda la nomina del DPO, come già sottolineato, l'art. 37 fa riferimento sia al titolare che al responsabile del trattamento di dati personali: ciò significa che il DPO potrà essere nominato solo dal titolare o solo dal responsabile, oppure potrà capitare che sia l'uno che l'altro siano obbligati, ed in questo caso entrambi i DPO saranno tenuti alla reciproca collaborazione[318].

La norma contiene poi ulteriori indicazioni relative alla nomina del DPO.

Viene precisato, infatti, che, nel caso in cui i trattamenti siano posti in essere dalle autorità pubbliche che agiscono a livello centrale e periferico, queste, tenuto conto della loro struttura organizzativa o dimensione, possano scegliere di nominare un unico DPO. Anche un gruppo imprenditoriale, inteso come gruppo costituito da un'impresa controllante e altre imprese da questa controllate, può scegliere di nominare un unico DPO, a condizione però che egli sia facilmente reperibile da ciascuno degli stabilimenti. Anche in relazione a questo profilo, le Linee guida si sono occupate di esplicare meglio il concetto di "reperibilità", chiarendo che lo stesso deve essere interpretato alla luce dei compiti che l'art. 39 GDPR affida al DPO: stante la funzione di contatto che il DPO esercita tanto nei confronti

[317] L'Autorità ha fornito altresì degli esempi utili all'interprete per individuare i tipi di trattamenti che sottopongono il titolare all'obbligo di nomina. Ad esempio, il trattamento dei dati relativi agli spostamenti degli utenti in un servizio di trasporto pubblico, il cui tracciamento avvenga attraverso titoli di viaggio; il trattamento dei dati da parte della struttura sanitaria (viceversa, non deve adempiere l'obbligo di nomina il singolo medico o operatore sanitario che tratta i dati dei pazienti); il trattamento dei dati relativi alla geolocalizzazione raccolti per finalità statistiche; il trattamento ad opera di una banca o di una compagnia assicurativa; il trattamento dei dati da parte di un motore di ricerca per finalità di pubblicità mirata sulla base delle preferenze.

[318] Il WP29, nelle Linee guida, a tal riguardo ha fornito alcuni esempi pratici di ipotesi in cui il titolare del trattamento potrebbe non essere obbligato alla nomina mentre, al contrario, il responsabile vi sarebbe tenuto. È il caso, ad esempio, di una piccola azienda a conduzione familiare operante nel settore della distribuzione di elettrodomestici che si serve di un responsabile del trattamento la cui attività principale consiste nel fornire servizi di tracciamento degli utenti del sito web oltre all'assistenza per attività di pubblicità e marketing mirati. In questo caso, poiché l'azienda non pone in essere un trattamento su larga scala, questa non sarà tenuta a nominare un DPO, mentre al contrario il responsabile del trattamento, che conta numerosi clienti simili all'azienda familiare, svolge, nel suo complesso, un trattamento su larga sala, da cui deriva l'obbligo di nominare un DPO.

dell'Autorità di controllo quanto dei soggetti interessati, nonché la necessità per lo stesso di comunicare e raffrontarsi con i vertici aziendali e gli addetti interni dell'impresa, è necessario che egli sia in grado di comunicare in modo efficiente, nella lingua o nelle lingue utilizzate nel luogo di stabilimento, in ciascuno degli stabilimenti. Alcune multinazionali, con stabilimento principale all'estero, hanno perciò deciso, sulla scorta della previsione in esame, di mantenere un unico DPO nel Paese di origine e di istituire degli uffici deputati alla gestione delle questioni relative alla protezione dei dati negli stabilimenti secondari collocati in altri Paesi, i quali sarebbero chiamati a relazionarsi con il DPO "centrale" solo in caso di necessità. Probabilmente, una soluzione del genere potrebbe considerarsi efficiente e non dispendiosa, tuttavia, i fattori problematici evidenziati in precedenza, nonché la necessità di una approfondita conoscenza della normativa specifica del singolo Stato membro in cui si colloca lo stabilimento secondario, suggerirebbero l'opportunità di nominare anche dei DPO "locali" in ciascuno degli stabilimenti[319]. Tale previsione, secondo il WP29, è ancor più necessaria nel caso in cui l'impresa (stabilimento) principale del titolare sia collocato in un Paese extra UE e abbia delle controllate nel territorio europeo.

6.2 La *vexata quaestio* in merito ai requisiti del *Data Protection Officer*

L'art. 37 GDPR, nel dettare la disciplina relativa alla designazione del DPO, indica, al paragrafo 5, quale requisito funzionale, le sue qualità professionali: in particolare, la legge pone l'accento sulla necessità, ai fini dell'assegnazione dell'incarico, di considerare la conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, nonché la capacità di assolvere i compiti di cui all'art. 39 GDPR.

La formulazione della disposizione, che si esprime in termini di clausole generali senza peraltro offrire alcun criterio di confronto o rinvio né indici di riferimento per una base maggiormente oggettiva dei criteri di selezione, ha determinato non poche incertezze nella dottrina, soprattutto negli ordinamenti che non vantavano esperienze precedenti con riferimento a tale figura professionale.

[319] Cfr. G. ZICCARDI, *GDPR, multinazionali: requisiti e ruolo del DPO unico*, 24 aprile 2018, reperibile al link *https://www.ipsoa.it/documents/impresa/contratti-dimpresa/quotidiano/2018/04/24/gdpr-multinazionali-requisiti-ruolo-dpo-unico*.

Ciò che il legislatore non prevede espressamente, ma che risulta essere un requisito imprescindibile, è il possesso di competenze specialistiche, ulteriori rispetto alla conoscenza ed alle competenze generiche, relative al settore in cui questi è chiamato ad operare.

In particolare, qualora si tratti, ad esempio di DPO operante alle dipendenze dei soggetti pubblici, il WP29 ha suggerito che questi dovrebbe avere competenza sulle norme e sulle procedure amministrative di riferimento. Oppure, nel caso in cui vengano posti in essere trattamenti transfrontalieri, sarà necessario che egli abbia competenza non solo in merito alla normativa e alle prassi nazionali, ma anche con riferimento alle normative vigenti negli altri Paesi verso i quali si attua il trasferimento di dati[320].

Peraltro, non può sottacersi la necessità, stante l'odierna natura e complessità delle attività di trattamento dei dati personali, che le conoscenze e competenze del DPO non siano limitate ai soli profili normativi, dovendo esse estendersi anche agli aspetti gestionali e tecnici della materia: in sostanza, l'esercizio della funzione di DPO richiede il possesso tanto di competenze "specialistiche" di carattere giuridico/amministrativo (e non limitate alla disciplina in materia di protezione dei dati personali), quanto di competenze "specifiche" relative alle modalità tecniche. La compresenza di tali competenze appare necessaria a

[320] In una nota dall'Ufficio del Garante italiano ad un'azienda ospedaliera, l'Autorità chiarisce, sulla scorta delle Linee guida del WP29, che "*se un trattamento riveste particolare complessità oppure comporta un volume consistente di dati sensibili, il RPD avrà probabilmente bisogno di un livello più elevato di conoscenze specialistiche e di supporto. Occorre anche distinguere in base all´esistenza di trasferimenti sistematici ovvero occasionali di dati personali al di fuori dell´Unione europea. Ne consegue la necessità di una particolare attenzione nella scelta del RPD, in cui si tenga adeguatamente conto delle tematiche in materia di protezione dei dati con cui il singolo titolare deve confrontarsi. Nel caso di un´azienda ospedaliera, la speciale complessità e delicatezza dei trattamenti di dati effettuati (dati sulla salute e dati genetici che costituiscono una categoria particolare di dati personali -art. 9, Reg. n. 2016/679) consiglia di privilegiare, nella selezione di questa figura, quella che può vantare una specifica esperienza al riguardo e assicurare un impegno pressoché esclusivo nella gestione dei trattamenti di questa tipologia di dati*". Nella selezione sarà, dunque, opportuno privilegiare soggetti che possano dimostrare qualità professionali adeguate alla complessità del compito da svolgere, magari documentando le esperienze fatte, la partecipazione a master e corsi di studio/professionali (in particolare se risulta documentato il livello raggiunto). Ciò, anche considerato che, nel caso di un'autorità pubblica o di un organismo pubblico, "*il RPD dovrebbe possedere una conoscenza approfondita anche delle norme e procedure amministrative che caratterizzano lo specifico settore, in quanto la liceità del trattamento dei dati personali in questo ambito dipende dalla corretta applicazione delle regole di volta in volta previste dalla disciplina speciale*". La nota (Doc-Web: 7057222 del 28.07.2017) è reperibile al link *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7057222*.

garantire, almeno sulla carta, una piena capacità del DPO per fronteggiare tanto le questioni legate alla *compliance* del titolare sul piano giuridico quanto quelle attinenti la *cybersicurezza* sul piano gestionale. È anche per tali ragioni che in dottrina è stato evidenziato come il DPO costituisca a tutti gli effetti espressione della doppia anima, giuridica e tecnica, che caratterizza l'intero sistema regolamentare in materia di protezione dei dati personali[321].

Alla luce di quanto sopra, si evince come il criterio discretivo cui attenersi nella scelta del miglior candidato, stante l'impossibilità di individuare (dal dato normativo) un livello minimo e preciso di competenza richiesto, debba essere basato sul possesso di un livello di competenza tanto più elevato quanto più complesse siano le attività di trattamento da porre in essere, ovvero quanto più sia elevato (quantitativamente) ed articolato il flusso di dati, eventualmente anche appartenenti alle categorie particolari ex art.9 , oggetto del trattamento[322].

Da tale lettura interpretativa deriva, tuttavia, un primo problema relativo alla acquisizione ed alla certificazione/attestazione del possesso delle competenze richieste; difatti posto che quella del DPO si presenta come una qualificazione professionale innovativa nel panorama italiano, ci si è chiesti attraverso quali canali le competenze richieste possano essere acquisite dai candidati alla posizione di DPO, e, ulteriormente, attraverso quali modalità di certificazione si possa dimostrare l'idoneità a ricoprire l'incarico in questione[323], non essendo richiesta una certificazione formale circa il percorso formativo ed il possesso delle conoscenze, né lo svolgimento di alcuna prova abilitativa, né tantomeno l'iscrizione ad appositi albi professionali: in relazione a questo ultimo profilo, peraltro, appare significativo evidenziare come non esista alcun albo o consiglio o ordine professionale con rilievo pubblico, dal momento che le uniche esperienze rintracciabili in Italia sono relative a forme associative di natura eminentemente

[321] C. SOLINAS, op. cit., p. 906.
[322] A. AVITABILE, op. cit., p. 345.
[323] Tali difficoltà, dunque, si pongono sia in relazione a coloro i quali, operando da tempo nel settore della *privacy*, abbiano già maturato una certa domestichezza con la normativa in materia di protezione dei dati, ma che ora - stante l'introduzione di istituti che richiedono conoscenze di carattere tecnico e informatico oltre che giuridico - si trovano ad avere necessità di un aggiornamento professionale di natura prettamente pratica, sia con riferimento a coloro i quali, volendosi affacciare a tale nuova professione, ma non avendo maturato alcuna esperienza nel settore, non abbiano la possibilità di entrare in possesso delle qualifiche richieste se non attraverso corsi di formazione mirati.

privata ed assolutamente circoscritte, quanto a diritti/doveri dei componenti e potere di rappresentanza della categoria, all'ambito interno, senza alcuna rilevanza esterna.

L'indeterminatezza dei criteri di selezione di riferimento potrebbe presentare dei risvolti negativi anche per il titolare, dal momento che la scelta e la nomina del DPO lo espongono, in caso di illecito con danni a terzi, ad una possibile contestazione in termini di *culpa in eligendo*, per la nomina di un soggetto che si dovesse dimostrare, in seguito, inidoneo a ricoprire l'incarico. Proprio in relazione al profilo della scelta ed alla determinazione dei criteri di selezione e valutazione, sembra configurarsi, a carico del titolare, una situazione di onere di diligenza e trasparenza, che peraltro potrebbe anche interpretarsi come una declinazione dello stesso principio di *accountability*. Il sistema delle responsabilità correlate all'operato del DPO, infatti, si riflette sul titolare e sulla posizione di garanzia che questi assume nei confronti dei soggetti interessati, ed al contempo degli eventuali altri operatori che entrino in contatto in ragione della circolazione dei dati (si pensi ad una impresa cessionaria di pacchetti di dati dall'originario titolare che si veda poi esposta a contestazioni in ragione delle originarie modalità di raccolta, trattamento e cessione). In caso di DPO interno (scelta che potrebbe essere giustificata nelle realtà di piccole dimensioni anche in forza di motivazioni economiche) il titolare assume, altresì, una posizione di garanzia anche nei confronti degli altri dipendenti, proprio in ragione dei criteri di trasparenza e di efficienza (aziendale) ai quali dovrebbe informare il proprio agire.

6.2.1 L'attività del *Data Protection Officer* deve essere certificata?[324]

L'indeterminatezza dei criteri indicati ha determinato il sorgere di una *vexata quaestio* circa la formazione del DPO, soprattutto in considerazione dell'assenza (almeno nel biennio 2016/2018), nell'ambito della formazione universitaria, di specifici percorsi o di una offerta mirata all'acquisizione delle competenze richieste.

[324] Il titolo di questo paragrafo prende spunto da un lavoro di E. LAUCHAD, *DPO certification should be regulated?*,
Maggio 10/2018), reperibile al link *https://ssrn.com/abstract=3176471*, o *http://dx.doi.org/10.2139/ssrn.3176471*.

Si è sviluppata, soprattutto in forza di una variegata offerta da parte di enti ed istituti privati, una articolata proposta di corsi di formazione (nelle diverse forme dei corsi di alta formazione, di master –non universitari-, di corsi di specializzazione), volti a promuovere l'acquisizione delle competenze richieste secondo le indicazioni fornite dalla legge e dalle linee guida sopra citate in merito ai requisiti che gli stessi debbano possedere. In un periodo successivo, anche le Università Statali hanno implementato la propria offerta formativa, giungendo anche ad istituire specifici corsi di studio in tema di diritto delle nuove tecnologie e tutela della persona.

In relazione ai percorsi formativi offerti dai privati già nei primi mesi successivi all'emanazione del GDPR, deve osservarsi che, nella maggior parte dei casi, tali corsi si sono rivelati inidonei ad una formazione proficua dei soggetti partecipanti, soprattutto per quanto riguarda il profilo pratico, essendosi spesso assestati su un piano prettamente teorico. Inoltre, l'analisi delle certificazioni rilasciate al termine della frequentazione degli stessi (spesso, ma non sempre, a seguito del superamento di un esame finale, disposto e gestito dall'ente proponente) ha dimostrato come l'offerta formativa sia stata variegata ed in alcuni casi assolutamente disomogenea, con contenuti assai differenti tra loro, determinando di conseguenza una frammentazione e talvolta una incongruità degli stessi rispetto alle effettive richieste di qualificazione professionale[325].

Sul punto non appare superfluo rilevare come la proliferazione di percorsi formativi incompleti od incongrui possa determinare la presenza, sul mercato, di una moltitudine si soggetti astrattamente in possesso di un attestato/certificato di qualificazione idoneo, ma, concretamente, non in possesso delle capacità di adempiere ai compiti richiesti, con conseguenti alterazioni del rapporto domanda/offerta e possibilità di scelte, da parte dei titolari, di soggetti non idonei.

La proliferazione dei percorsi formativi, in un mercato sempre più assetato di nuovi sbocchi professionali, non sarebbe, di per sé, un fattore negativo poiché,

[325] Mentre alcuni programmi di formazione rilasciano un certificato di partecipazione senza che vi sia alcuna valutazione finale dei candidati, altri rilasciano il certificato di partecipazione solo agli studenti che non siano riusciti a superare l'esame finale, altrimenti viene rilasciato un vero e proprio certificato di idoneità. Quest'ultimo, a sua volta, potrà avere validità temporalmente limitata, oppure non avere scadenza. Ovviamente tutto ciò contribuisce alla confusione esistente circa la natura e il valore delle certificazioni rilasciate dai differenti organismi che agiscono sul mercato.

anzi, in base al libero gioco della concorrenza, potrebbe indurre gli operatori ad attuare una corsa al miglioramento dell'offerta; purtroppo, la declinazione patologica del fenomeno risiede nella proliferazione di una offerta non sempre qualificata, ed indirizzata, talvolta, alla concorrenza sul profilo economico e non qualitativo/contenutistico: il gioco della concorrenza si sposta sull'offerta economicamente più vantaggiosa, anche a scapito della completezza del percorso formativo.

Vengono così a determinarsi difformi livelli di competenza dei (potenziali) DPO, che trovano la propria base solo con riferimento ad un blocco di competenze basilari e imprescindibili. Sul portato di queste considerazioni, appare auspicabile un intervento del legislatore per offrire indicazioni, vincolanti per tutti gli operatori, sui contenuti minimi dei programmi formativi e sulle modalità di accertamento delle competenze raggiunte, con rilascio di certificazioni uniformi, con pieno valore legale dei livelli di qualificazione raggiunti[326].

Stante la situazione attuale, tuttavia, le certificazioni/attestazioni rilasciate all'esito di tali corsi (erogati da Università e Centri di ricerca statali come da operatori e formatori privati) rappresentano, al pari di altri titoli, uno strumento utilizzabile per valutare il possesso di un livello minimo di conoscenza della disciplina, sebbene le stesse non equivalgano, di per sé, ad una abilitazione allo svolgimento del ruolo di DPO, né possano sostituire in toto la valutazione dell'azienda, dell'ente o della P.A. nell'analisi e valutazione del possesso dei requisiti necessari per svolgere i compiti da assegnare al DPO in conformità all´art. 39 del GDPR[327].

Proprio per le ragioni esposte, molti professionisti avevano avanzato l'idea che, per coloro che avessero voluto ricoprire il ruolo di DPO, si dovesse rendere obbligatoria la certificazione rilasciata sulla base della Norma UNI 11697:2017[328]

[326] E. LACHAUD, op. cit.

[327] V. nota del Garante per la protezione dei dati personali (Doc-Web: 7057222 del 28.07.2017), cit.

[328] Le norme UNI sono documenti che definiscono le caratteristiche (dimensionali, prestazionali, ambientali, di qualità, di sicurezza, di organizzazione ecc.) di un prodotto, processo o servizio, secondo lo stato dell'arte, e sono il risultato del lavoro di migliaia di esperti del settore di riferimento. Le caratteristiche peculiari delle norme tecniche sono:

- consensualità: deve essere approvata con il consenso di coloro che hanno partecipato ai lavori;

relativa alle "attività professionali non regolamentate – Profili professionali relativi al trattamento e alla protezione dei dati personali – Requisiti di conoscenza, abilità e competenza"[329]. Con la norma UNI 11697:2017, sulla scorta di quanto previsto dal GDPR, sono stati ulteriormente dettagliati i requisiti relativi

---

- democraticità: tutte le parti economico/sociali interessate possono partecipare ai lavori e, soprattutto, chiunque è messo in grado di formulare osservazioni nell'iter che precede l'approvazione finale;
- trasparenza: UNI segnala le tappe fondamentali dell'iter di approvazione di un progetto di norma, tenendo il progetto stesso a disposizione degli interessati;
- volontarietà: le norme sono un riferimento che le parti interessate si impongono spontaneamente.

L'iter che porta alla nascita di una norma si articola in diverse fasi: la messa allo studio, la stesura del documento, l'inchiesta pubblica, l'approvazione da parte della Commissione Centrale Tecnica e la pubblicazione.

Le definizioni di cui sopra sono state tratte dal sito dell'UNI (ente nazionale di normazione), per cui si rinvia al link *http://www.uni.com/index.php?option=com_content&view=article&id=361&Itemid=2445*.

Sul sito dell'UNI è stato altresì chiarito che "*con l'approvazione della Legge n. 4 del 14 gennaio 2013 "Disposizioni in materia di professioni non organizzate", l'attività di normazione UNI ha assunto ulteriore rilevanza. Infatti, la legge dà piena applicazione al principio di sinergia tra legislazione e normazione tecnica. In particolare, l'articolo 6 "Autoregolamentazione volontaria", pur non rendendo obbligatorio il rispetto delle norme UNI, definisce quei principi e criteri generali che disciplinano l'esercizio autoregolamentato dell'attività professionale che la norma tecnica di fatto garantisce. Così la conformità alle norme UNI e la partecipazione ai lavori degli organi tecnici (di cui all'articolo 9 "Certificazione di conformità a norme tecniche UNI") diventano un fattore determinante*". V. al link *http://uni.com/index.php?option=com_content&view=article&id=1621:normazione-e-professioni-non-regolamentate&catid=150:normazione&Itemid=2456*.

[329] La norma UNI 11697:2017, frutto di una collaborazione dichiarata dal principio tra esperti legali ed esperti di ICT provenienti dalle commissioni UNI "Servizi" e "Sicurezza della società e del cittadino" e dalla commissione UNINFO "APNR – ICT", recepisce pienamente non solo le disposizioni in materia del Regolamento UE 2016/679 ma anche tutte le più recenti indicazioni fornite dal WP29 mettendo insieme le conoscenze delle diverse componenti di maggior rilievo delle norme di legge applicabili e quelle dei sistemi informativi, nonché delle tecniche di protezione e sicurezza ad essi relative, ormai imprescindibili nella nostra società. È stato definito un insieme "minimo" di profili professionali che, assieme ad una figura di DPO allineata alla lettera ai dettami del nuovo Regolamento UE 2016/679, include una figura di taglio manageriale, una figura di tipo operativo e una figura di valutatore esterno:

- Responsabile della protezione dei dati personali (DPO): figura di supporto al Titolare o Responsabile del trattamento nell'applicazione del regolamento e per l'osservanza del Regolamento (UE) 2016/679 in conformità agli artt. 37-39.
- Manager *privacy*: figura che assiste il Titolare del trattamento nel coordinamento dei soggetti coinvolti nel trattamento dei dati personali, al fine di garantire il rispetto delle norme di legge applicabili e il raggiungimento nonché il mantenimento del livello di protezione adeguato in base allo specifico trattamento di dati personali effettuato.
- Valutatore *Privacy*: figura indipendente con conoscenze e competenze nel settore informatico/tecnologico e di natura giuridica/organizzativa (che abbia una formazione minima di 40 ore) che conduce attività di audit sulla conformità dei trattamenti di dati personali avvalendosi, se necessario, di specialistici in entrambi gli ambiti.
- Specialista *Privacy*: figura "operativa" che supporta il DPO e/o il Manager *Privacy* nel mettere a punto idonee misure tecniche e organizzative ai fini del trattamento di dati personali e cura la corretta attuazione del trattamento di dati personali.

V. *link https://www.federprivacy.org/formazione/Privacy_Officer_CNR_Storia_Evoluzione.pdf* .

ai professionisti chiamati ad operare nell'ambito del trattamento dei dati personali, tra cui, in conformità agli artt. 37-39 GDPR, anche i requisiti del DPO.

In relazione a tale figura, la norma richiede al professionista che voglia ottenere la certificazione una laurea, un corso di formazione di almeno 80 ore su "*Gestione della Privacy e Sicurezza delle Informazioni*" con attestazione finale, e un minimo di sei anni di esperienza lavorativa legata alla *privacy*, di cui almeno quattro anni in incarichi manageriali (gli anni possono diminuire o aumentare in funzione del titolo di studio – laurea magistrale o diploma). In possesso di tali requisiti, il soggetto interessato potrà partecipare ad un esame composto da test a risposta multipla, una prova a risposta aperta ed un esame orale in cui deve sostenere un *role-play*, vale a dire la simulazione di situazioni reali: solo al superamento dei suddetti esami potrà ottenere la certificazione.

Sul punto, Federprivacy[330], la principale associazione professionale in Italia di Privacy Officer e addetti ai lavori della data protection, ha richiesto al Garante dei chiarimenti circa l'obbligatorietà o meno di tale certificazione, basata sulla norma UNI 11697:2017, da parte di coloro che intendano lavorare in qualità di DPO. Con nota Prot. n. 9530/2018 del 27 marzo 2018 indirizzata a detta associazione, il Garante ha specificato che tale certificazione non rientra tra quelle disciplinate dall'art. 42 del GDPR, quindi non può essere approvata né dalla stessa Autorità di controllo italiana, né dal Comitato europeo per la protezione dei dati, e dunque non è da ritenersi obbligatoria.

Inoltre, in considerazione della mancanza di un obbligo di certificazione per coloro i quali vogliano ricoprire tale incarico, deriva ulteriormente che gli stessi possano ricorrere anche all'acquisizione di certificazioni non necessariamente basate sulla predetta norma, potendo invece essere basate su altri schemi proprietari[331]. L'Autorità, infatti, ha chiarito che tutte le certificazioni rappresentano, al pari di altri titoli, semplicemente "uno strumento per dimostrare

[330] Costituita nel 2008, Feder*privacy* è la principale associazione professionale in Italia di *Privacy Officer* e addetti ai lavori della *data protection*, iscritta nel Registro del Ministero dello Sviluppo Economico ai fini della Legge 4/2013. Dal 2011, Feder*privacy* ha promosso la certificazione delle competenze della figura professionale del "*Privacy* Officer e Consulente della *Privacy*" basata sul proprio disciplinare, che viene rilasciata dal Tüv Examination Institute.

[331] In assenza di una norma tecnica UNI che definisca univocamente la professione, è consentito realizzare uno schema di certificazione di persone, definito schema proprietario, costruito sulla base di requisiti individuati da parti interessate alla professione (associazioni professionali, utenti, enti di studio, etc.)

il possesso da parte del professionista delle conoscenze, competenze e abilità necessarie allo svolgimento dello specifico ruolo".

Le certificazioni, dunque, specialmente se rilasciate da enti indipendenti di terza parte, potranno costituire, secondo il Garante, un valido strumento ai fini della verifica del possesso di un certo livello di conoscenza della disciplina, mantenendo però pur sempre il proprio carattere di certificazioni acquisite volontariamente, e mai obbligatorie, sia che siano basate su norme tecniche pubbliche che su schemi proprietari.

Certo è che, sebbene non obbligatorie, le certificazioni basate sulla norma UNI 11697:2017 potrebbero essere considerate di maggior pregio e valore rispetto alle altre: chi possiede le prime, infatti, dimostra non solo di avere una formazione teorica forte, ma anche idonee competenze di carattere tecnico-informatico, grazie alle quali ha superato un esame finale articolato.

Ciò consentirebbe al titolare che si affida ai professionisti certificati ai sensi della norma tecnica, di poter provare, in caso di eventuali controlli, di avere agito, in sede di designazione e selezione, nel rispetto del principio di *accountability*, affidandosi a soggetti che posseggono tutte le competenze necessarie a guidarli nel loro operato.

Qualora, invece, il titolare o responsabile selezionassero e/o designassero professionisti che hanno ottenuto certificazioni/attestazioni basate su schemi volontari, dal momento che tali certificazioni presentano pur sempre un contenuto variabile, al fine di informare la propria scelta al principio di *accountability*, essi saranno tenuti ad effettuare una più approfondita analisi e valutazione circa le competenze certificate ed effettivamente possedute.

In relazione a quanto detto, emerge una amara considerazione, cioè che, in ogni caso, resterebbero comunque esclusi dal beneficio offerto dal possesso della certificazione tutti quei candidati più giovani, sia dal punto di vista anagrafico che lavorativo, che non hanno potuto maturare un’esperienza di carattere pratico nel settore di riferimento, ma che, dal punto di vista teorico, risultano preparati, magari anche grazie alla partecipazione a corsi specializzanti in materia.

Il silenzio del GDPR sulla formazione dei DPO ha permesso alle legislazioni dei singoli Stati membri di operare secondo differenti criteri di valutazione: se, come

visto, in Italia non sono state date ulteriori indicazioni in merito, pur se sarebbe auspicabile un intervento del legislatore o dell'Autorità di controllo, in altri ordinamenti si è proceduto alla indicazione di criteri e requisiti precisi.

Stante le considerazioni svolte, appare utile, a sostegno di una possibile modifica della disciplina normativa inerente le certificazioni, analizzare da vicino quanto disposto dal legislatore spagnolo. In Spagna, infatti, l'Autorità di controllo pubblica, la *Agencia Española de Protección de Datos* (AEPD), per far fronte all'esigenza di una certificazione unitaria, ha creato uno schema di certificazione per coloro che vogliano diventare DPO, che potrà essere utilizzato da tutti gli enti accreditati per il rilascio delle certificazioni. L'Autorità ha delineato nel dettaglio i contenuti dei compiti del DPO, gli obiettivi che lo stesso deve perseguire, le competenze specifiche e il *know-how* che deve possedere al fine di ottenere la certificazione.

Gli aspetti rilevanti di tale prassi sono almeno due. Un primo aspetto è certamente quello relativo al ruolo dell'Autorità di controllo, che predispone i contenuti della certificazione che deve essere rilasciata dagli enti accreditati (l'Autorità pubblica interviene, accanto al legislatore, definendo, ancor più nel dettaglio, i requisiti imprescindibili che devono essere comuni ad ogni DPO che voglia dotarsi della certificazione); sebbene non sia l'Autorità a rilasciare le certificazioni in questione, è tuttavia evidente come attraverso la predisposizione di tale schema, la stessa eserciti un'influenza notevole che si riflette non solo sulle altre certificazioni eventualmente esistenti, ma, indirettamente, finanche sulla stessa natura dell'incarico. La portata di tale intervento si può comprendere pienamente allorché si ragioni sulla circostanza per cui, potenzialmente, ogni candidato alla posizione di DPO avrà certamente interesse ad ottenere la relativa certificazione, al fine di essere assunto dal titolare, ed una certificazione rilasciata sulla base dei requisiti predisposti dall'Autorità pubblica avrà sicuramente un valore superiore rispetto ad altre certificazioni, anche se egualmente (astrattamente) considerabili. Tale intervento autoritativo determina dei riflessi sul ruolo in esame, che sembrerebbe venire ad assumere un rilievo con profili quasi pubblicistici, più in linea con il tipo di interesse che il DPO è chiamato a tutelare.

Un ulteriore rilievo, di non poco significato, concerne i requisiti individuati dall'Autorità, che il candidato deve possedere per poter accedere alla fase di valutazione e ottenere la certificazione. Viene, infatti, richiesto che il candidato possegga uno dei seguenti requisiti:

1) abbia maturato un'esperienza professionale di almeno cinque anni in progetti, attività o compiti collegati con le funzioni del DPO, in materia di protezione dei dati;

2) abbia maturato un'esperienza professionale di almeno tre anni in progetti, attività o compiti collegati con le funzioni del DPO, in materia di protezione dei dati, e una formazione minima riconosciuta di 60 ore in materie incluse nel programma dello schema;

3) abbia maturato un'esperienza professionale di almeno due anni in progetti, attività o compiti collegati con le funzioni del DPO, in materia di protezione dei dati, e una formazione minima riconosciuta di 100 ore in materie incluse nel programma dello schema;

4) abbia maturato una formazione minima riconosciuta di 180 ore in materie incluse nel programma dello schema.

Risalta immediatamente come l'Autorità abbia deciso di porre sullo stesso piano gli anni di esercizio effettivo della professione e le 180 ore di formazione teorica: tale decisione ha il pregio di consentire anche a coloro i quali non abbiano potuto maturare alcuna esperienza sul campo di poter ottenere la certificazione. C'è chi ha criticato profondamente questa scelta, giudicando la stessa "ridicola" e ritenendo che l'Autorità, così disponendo, abbia preferito ragionare su termini quantitativi piuttosto che qualitativi: 180 ore di formazione costituirebbero, secondo tale dottrina, il minimo indispensabile per imparare soltanto le regole idonee a svolgere una valutazione d'impatto[332].

Certamente, la via perseguita nell'ordinamento spagnolo presenta dei *pro* e dei *contro*, ma ha senza dubbio il pregio di aver per lo meno introdotto la possibilità di individuare un insieme di requisiti minimi necessari ai fini dello svolgimento dell'attività di DPO, salvaguardando, al contempo, l'interesse dei titolari/responsabili e quello degli interessati, posto che, a presidio e controllo

[332] R. MARTINEZ, op. cit., pp. 456-458.

delle attività di trattamento , vi è un soggetto che appare preparato a fronteggiare i rischi cui il trattamento si espone.

6.2.2 La sentenza del TAR Friuli Venezia Giulia del 13 settembre 2018, n. 287

L'indeterminatezza in ordine ai criteri di selezione ed alle modalità di valutazione dei requisiti richiesti ai potenziali candidati per ricoprire l'incarico di DPO, ha determinato l'emergere di una serie di contestazioni, approdate alle sedi giudiziarie, in ordine soprattutto alle procedure relative alla selezione per incarichi presso enti pubblici.

Preliminarmente occorre infatti ricordare che, nel settore privato, stante l'assenza di indicazioni vincolanti *ex lege*, i criteri della selezione/designazione sono rimessi alla discrezionalità del titolare (o del responsabile), con gli unici vincoli di invalidità delle clausole del bando di selezione che risultassero discriminatorie o invasive/lesive della sfera privata della persona (si pensi a clausole limitative di genere, o di vincoli ai diritti dei lavoratori genitori, od ancora limitative delle scelte personali di vita e di coscienza).

In riferimento ai bandi di selezione per l'incarico di DPO presso ente pubblico, invece, si sono poste alcune questioni sulle quali la giurisprudenza dei TAR ha offerto alcuni interessanti spunti di riflessione.

In particolare, si consideri la decisione del TAR del Friuli Venezia Giulia in materia di formazione del DPO, resa con sentenza del 13 Settembre 2018[333] che, a detta di molti commentatori, inaugura quello che potrà diventare un filone giurisprudenziale attinente le questioni giuridico-interpretative aventi ad oggetto il ruolo del *Data Protection Officer*.

La vicenda sottoposta alla cognizione del TAR aveva ad oggetto un ricorso presentato avverso l'avviso pubblico prot. n. 16546 del 5.4.2018, con il quale l'Azienda per l'assistenza sanitaria n. 3 del Friuli bandiva l'affidamento di un incarico di collaborazione professionale per l'impostazione e lo svolgimento dei compiti di DPO. Rilevata l'assenza, tra i propri dipendenti, di una figura professionale idonea a svolgere l'incarico in questione, era stata prevista la selezione, per titoli ed eventuale colloquio, di un esperto di normativa e prassi in

[333] TAR Friuli Venezia Giulia, sez. I, sentenza 5 – 13 settembre 2018, n. 287.

materia di protezione dei dati. Nel bando, dopo aver indicato i compiti che il soggetto vincitore della selezione sarebbe andato a svolgere in qualità di DPO, al paragrafo 3, venivano elencati i requisiti indispensabili ai fini della partecipazione alla selezione. Nello specifico, veniva richiesto il possesso, in capo a ciascun candidato, del diploma di laurea in Informatica o Ingegneria Informatica, ovvero in Giurisprudenza o equipollenti, nonché la certificazione di *Auditor/Lead Auditor* per i Sistemi di Gestione per la Sicurezza delle Informazioni secondo la norma ISO/IEC/27001.

Occorre sin d'ora rilevare che la norma ISO/IEC/27001 (Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti) è una norma tecnica di carattere internazionale (che si distingue da quella UNI, di rilevanza nazionale), che definisce i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni, e riguarda gli aspetti relativi alla sicurezza logica, fisica ed organizzativa dei sistemi. Si tratta della norma tecnica più famosa al mondo avente ad oggetto la gestione delle informazioni aziendali.

Il ricorrente, all'atto di richiesta di partecipazione alla selezione, produceva vari titoli curriculari, tra cui la laurea in Giurisprudenza, dichiarando tuttavia di non possedere la certificazione richiesta. A tal riguardo precisava che "la certificazione indicata quale requisito non appare pertinente, sia perché l'ASUIUD[334] e l'AAS3[335] non possiedono la certificazione ISO/IEC/27001, sia perché la norma è antecedente rispetto all'emanazione del GDPR e, quindi, il diploma di Auditor/Lead Auditor non può essere una certificazione rilevante per un esperto di normativa e prassi da nominare quale DPO".

Senza attendere le determinazioni dell'Amministrazione, il ricorrente proponeva l'immediata impugnazione dell'avviso pubblico, rilevando la violazione degli artt. 37 e 39 del Reg. UE n. 679/2016 nonché l'eccesso di potere con riferimento alla violazione di atti di regolazione; la violazione di atto presupposto; la manifesta illogicità ed irrazionalità dei requisiti di partecipazione alla selezione.

[334] L'abbreviazione sta per "*Azienda Sanitaria Universitaria Integrata di Udine*".
[335] L'abbreviazione sta per "*Azienda per l'Assistenza Sanitaria n. 3 Alto Friuli Collinare Medio Friuli"*.

In particolare, il ricorrente contestava la richiesta, tra i requisiti utili ad ottenere l'incarico, del possesso della certificazione Auditor/Lead Auditor ISO/IEC/27001, ritenendo che tale titolo, poiché privo di attinenza riguardo alle mansioni specificamente richieste dal GDPR e agli ultronei compiti enunciati nell'avviso, determinerebbe un'indebita sperequazione a danno delle persone laureate (in Giurisprudenza o Informatica) ma non in possesso della richiamata certificazione. *Sub specie*, il ricorrente evidenziava il dubbio interpretativo circa la necessità del possesso di tale certificazione quale requisito alternativo a quello della laurea ovvero ulteriore ad essa (considerata la presenza della congiunzione "nonché"). Inoltre, contestava la scelta di ammettere alla selezione i laureati in Ingegneria/Informatica, evidenziando che le competenze necessarie per lo svolgimento dell'incarico non possono essere ricondotte alla laurea in Informatica o in Ingegneria informatica, e ritenendo che il profilo professionale oggetto della selezione possa essere ricoperto soltanto da un laureato in giurisprudenza.

In seguito, con motivi aggiunti, il ricorrente impugnava il successivo verbale adottato con decreto del Direttore Generale, con cui veniva designato quale Responsabile per la protezione dei dati l'altro (unico) candidato. In particolare, la commissione specificava, nel verbale, di non ritenere ammissibile la candidatura presentata dal ricorrente, proprio in virtù del mancato possesso della certificazione ISO/IEC/27001.

Il Giudice, dopo aver rigettato le eccezioni di rito[336], pronunciandosi nel merito, sanciva che il possesso della richiesta certificazione ISO/IEC/27001, di per sé,

[336] Le eccezioni presentate dalla resistente erano relative al difetto di giurisdizione del Giudice Amministrativo, a favore di quello ordinario. Il TAR ha rilevato che, poiché "*l'oggetto della controversia attiene all'assegnazione di un incarico, mediante l'espletamento di una selezione comparativa, direttamente riconducibile ad esigenze proprie dell'Amministrazione, connesse all'esercizio di funzioni istituzionali (tra le quali devono essere incluse le competenze e le responsabilità in tema di protezione dei dati, introdotte e regolate dal GDPR)*", la giurisdizione appartiene al giudice amministrativo, stante l'orientamento delle Sezioni Unite in virtù del quale "a*ppartiene alla giurisdizione del giudice amministrativo la controversia relativa ad una procedura concorsuale volta al conferimento di incarichi ex art. 7, comma 6, d.lg. n. 165 cit., assegnati ad esperti, mediante contratti di lavoro autonomo di natura occasionale o coordinata e continuativa, per far fronte alle medesime esigenze cui ordinariamente sono preordinati i lavoratori subordinati della p.a.*" (Cass. S.U. n. 13531 del 2016). La seconda eccezione era relativa alla carenza di interesse del ricorso e dei motivi aggiunti. Il TAR a tal riguardo ha osservato che "*il ricorrente, in quanto soggetto partecipante alla procedura, risulta portatore di un interesse sufficientemente differenziato inteso a conseguire la corretta interpretazione ed applicazione della disciplina regolatrice della selezione nei propri confronti*". Il fine ultimo del ricorrente è, infatti, quello di delimitare il perimetro dei soggetti ammessi e a depotenziare i titoli

non può costituire requisito di ammissione alla selezione in esame (né tanto meno assurgere a titolo equipollente al richiesto diploma di laurea). Tale certificazione, infatti, non può essere considerata quale titolo abilitante ai fini dell'assunzione e dello svolgimento delle funzioni di Responsabile della sicurezza dei dati, in considerazione della circostanza per cui, da un lato, la norma ISO 27001 trova prevalente applicazione nell'ambito dell'attività di impresa, e non del settore pubblico (che è il caso che qui interessa)[337]; dall'altro lato, "la medesima norma, per quanto potenzialmente estensibile all'attività delle pubbliche amministrazioni, fa pur sempre salva l'applicazione delle disposizioni speciali (euro-unitarie e nazionali) in materia di tutela dei dati personali e della riservatezza (punto 18 "conformità" della citata norma ISO; cfr. in particolare: 18.1.1 e 18.1.4), 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"[338].

Sul punto, il Giudice chiarisce che la certificazione in questione non coglie (o non coglie a pieno) la specifica funzione di garanzia insita nell'incarico di DPO, il cui precipuo oggetto non è la predisposizione di meccanismi volti ad incrementare i livelli di efficienza e di sicurezza nella gestione delle informazioni, ma, più estensivamente, attiene alla tutela del diritto fondamentale dell'individuo alla protezione dei dati personali: la predisposizione degli strumenti idonei a garantire tale tutela costituisce solo uno degli aspetti attraverso il quale si realizza il compito del DPO, ma non certo l'unico. In ragione di tali circostanze, si afferma che il DPO deve possedere delle conoscenze ulteriori e più specifiche di quelle attestate dalla certificazione basata sulla norma ISO 27001[339].

---

curriculari da questi eventualmente allegati, con ciò ampliando le possibilità di assegnazione dell'incarico. Cfr. sent. TAR Friuli Venezia Giulia 13 settembre 2018 n. 287.

[337] Si legge al riguardo nella sentenza "*basti rilevare che i riferimenti rivolti ad essa* [certificazione ISO 27001]*, dal legislatore nazionale e dall'ordinamento euro-unitario, attengono essenzialmente ai requisiti degli operatori economici, come ad esempio avviene nel caso dell'art. 93, comma 7, D. Lgs. n. 50 del 2016, in tema di garanzie per la partecipazione alle procedure di affidamento nei settori ordinari*". Ibidem, p. 4.1.1 e 4.1.2

[338] Ibidem, p. 5.

[339] Il Giudice prosegue "*Tali conclusioni sono ulteriormente rafforzate dall'esame dei programmi dei corsi finalizzati all'acquisizione della certificazione ISO/IEC/27001, caratterizzati da una*

Alla luce delle considerazioni svolte, il TAR esclude, pertanto, che dal possesso della certificazione in esame possa essere fatta dipendere l'ammissione alla procedura selettiva, trattandosi, a ben vedere, di un mero titolo curriculare, certamente valutabile in sede di giudizio sulle posizioni dei singoli candidati, ma non anche di un titolo formativo o abilitante, come tale idoneo ad assurgere a requisito di accesso.

A sostegno di quest'orientamento, il Giudice rileva altresì che l'Azienda, nelle more del giudizio, ha incaricato dello svolgimento dei compiti di DPO i propri dirigenti, i quali risultavano carenti proprio della certificazione ISO/IEC/27001.

La sentenza in esame costituisce un interessante ed utilissimo spunto ai fini dell'interpretazione dell'art. 37 GDPR, per due ordini di ragioni. La prima, che si pone in linea con quanto già evidenziato dal Garante, riguarda la conferma della non obbligatorietà del possesso di certificazioni idonee a comprovare le competenze in materia di data protection, sia che si tratti di certificazioni nazionali, sia che si tratti di quelle internazionali. La seconda, invece, riguarda la presa di posizione del TAR a favore del profilo giuridico del DPO. La motivazione della sentenza, nel passaggio in cui indica che il profilo del DPO "non può che qualificarsi come eminentemente giuridico", deve essere intesa non già nel senso di limitare l'esercizio della professione esclusivamente agli operatori del diritto ma, invero, nel senso che, a prescindere dal titolo di studio, il DPO debba necessariamente possedere competenze di carattere giuridico, così come già specificato dal WP29. Del resto, nella maggior parte dei casi, le aziende hanno già al loro interno delle figure in grado di sopperire alle esigenze tecniche, mentre spesso mancano figure legali specializzate in materia di protezione dei dati personali.

È chiaro, altresì, che il DPO dovrà in ogni caso implementare ulteriori conoscenze, di carattere tecnico e informatico[340], data la complessità delle

---

durata particolarmente contenuta (2/5 giorni), per un massimo di 40 ore, dalla netta prevalenza delle tematiche attinenti all'organizzazione aziendale (e ciò a discapito dei profili giuridici) e dall'assenza di contenuti riferibili all'attività e alla struttura delle pubbliche amministrazioni" Ibidem, p. 5.

[340]È necessario che il DPO conosca le tecnologie rilevanti ed utili nell'ambito dei trattamenti, come, a titolo esemplificativo, i servizi di *cloud storage*, *data lakes*, *I.o.T.*, *A.I.*, *blockchain* e *smart contracts*, anche al fine di assicurare la sicurezza e la resilienza dei sistemi informatici in modo da evitare quanto più possibile rischi di attacchi ai suddetti sistemi (*data breach)*.

problematiche che possono venire in rilievo e rispetto alle quali egli dovrà fornire soluzioni di carattere più pratico che teorico; nonché in considerazione della necessità di poter scientemente confrontarsi con gli addetti ai sistemi informatici.

Da tale sentenza, ed in generale dall'analisi sin qui svolta emerge, dunque, con evidenza, la scelta del legislatore di non condizionare l'accesso alla professione al possesso di un titolo specifico ed ultroneo rispetto alla laurea (preferibilmente in materie giuridiche), idoneo a comprovare il possesso di determinate competenze in materia di protezione dei dati personali.

In relazione alla scelta del legislatore, avallata come visto dalla giurisprudenza, permangono alcune perplessità.

Premesso che non può che condividersi la scelta del TAR di non riconoscere come vincolante il possesso di una certificazione inerente qualificazioni meramente tecniche, resta il dubbio sulla possibilità di richiedere una certificazione attestante il possesso delle conoscenze e competenze di carattere giuridico.

Sul punto, sebbene tale scelta, possa essere spiegata in considerazione del fatto che il DPO sia chiamato a svolgere un ruolo a servizio dell'interesse del titolare (sarà pertanto specifico interesse di quest'ultimo individuare il soggetto più competente a coadiuvarlo nella sua azione) appare utile sottolineare che procedura di certificazione potrebbe offrire almeno tre benefici:

1) Verificare la sussistenza delle competenze richieste;

2) Garantire la conformità dell'attestazione per i candidati, per un periodo di tempo delimitato, ossia fin quando i requisiti sono effettivamente presenti, potendo poi essere rinnovata a seguito di eventuale nuovo esame;

3) Aiutare il titolare del trattamento ad essere considerato effettivamente *compliant* rispetto alla normativa, poiché questi potrà avvalersi di un soggetto realmente idoneo a garantire il rispetto del diritto alla protezione dei dati personali[341].

[341] L'elencazione dei benefici del processo certificatorio era già stata proposta da E. LAUCHAD, *DPO certification should be regulated*, op. cit. Tuttavia, sebbene si ritiene di poter essere d'accordo sui primi due punti, con riferimento al terzo si è scelto di individuarne uno differente rispetto a quello riscontrabile nel lavoro sopracitato. Lauchad, infatti, sostiene che "*it helps at monitoring the compliance over time insofar as the applicant is required, at the end of the validity*

Ed ancora, accanto alle ragioni esposte, ne emerge una ulteriore. Infatti, in considerazione del ruolo chiave che il DPO gioca ai fini della tutela del fondamentale interesse alla protezione dei dati personali, dovrebbe ritenersi necessario per le aziende private e per enti pubblici potersi dotare di soggetti realmente idonei a ricoprire l'incarico in esame, e tale idoneità verrebbe appunto assicurata dal possesso di una certificazione rilasciata da formatori pubblici e privati, ma su programmi e modelli determinati ex lege o dall'Autorità Garante; ancora meglio, dallo stesso EDPB con un modello di certificazione unica, valida in tutti gli Stati membri [342].

6.3 Le prerogative del *Data Protection Officer*

Proseguendo nell'analisi dei profili inerenti la nomina e, più in generale, la funzione del DPO, particolare attenzione merita il par. 6 dell'art. 37 GDPR, ove viene sancito che l'incarico possa essere svolto sia da un soggetto interno all'organizzazione (dipendente del titolare del trattamento), sulla base di un atto di designazione, sia da un soggetto esterno, sulla base di un apposito contratto di servizi.

In entrambi i casi, sarà necessario che l'incaricato sia autonomo e indipendente rispetto al titolare, come emerge dalla lettura del successivo art. 38[343], nel quale vengono dettate alcune regole fondamentali da rispettare nell'ambito del rapporto intercorrente tra il titolare (o responsabile) e il DPO, al fine di garantire l'autonomia e l'indipendenza di quest'ultimo.

L'art. 38, al paragrafo 1, dispone che il titolare ed il responsabile del trattamento coinvolgano tempestivamente e adeguatamente il DPO in tutte le questioni riguardanti la protezione dei dati personali. È necessario, dunque, che sia garantito un flusso costante di informazioni biunivoco: non solo da parte del titolare e del responsabile verso il DPO (ad esempio nel caso in cui dovessero insorgere nuovi

---

period, to voluntarily and successfully renew a conformity assessment to keep the benefit of its certification".

[342] La Commissione europea, a tal fine, potrebbe creare uno schema certificatorio da concedere in licenza ad organismi di certificazione privati accreditati, al fine di garantire la coerenza e l'uniformità dei requisiti richiesti.

[343] Viene, altresì, in rilievo il considerando 97, che aggiunge che i DPO "*dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente".*

rischi nell'ambito del trattamento di dati, o si dovesse dare l'avvio a trattamenti nuovi), ma anche da parte del DPO nei confronti di titolare e responsabile (ad esempio nel caso in cui venga a conoscenza di misure più idonee a garantire una maggior tutela dei soggetti interessati).

Proprio perché al DPO deve essere garantito l'accesso a tutte le informazioni utili per l'espletamento dei propri compiti, l'obbligo di rendere disponibili dati, documenti, e qualunque altra informazione il DPO richieda, dovrà gravare su qualunque dipendente, ed il DPO dovrà riferire al titolare di eventuali condotte negligenti di questi ultimi, nel caso in cui dovesse venirne a conoscenza. In tal senso, sarebbe opportuno inserire nel regolamento interno all'azienda la previsione di sanzioni in caso di violazioni di tale obbligo.

Ancora, è previsto che il titolare o il responsabile forniscano al DPO ogni risorsa necessaria per l'esercizio delle sue funzioni, e per garantirne l'aggiornamento professionale. Ciò significa che, anche nell'ipotesi in cui l'incarico venga affidato a un soggetto interno, il titolare debba disporre una forma di compenso specifico in suo favore. Sarebbe preferibile che al DPO venga offerto un compenso non variabile, che possa coprire l'intera durata dell'incarico, e che venga determinato facendo riferimento ad alcuni elementi quali, ad esempio, la complessità e la quantità dei trattamenti di dati personali posti in essere, ma anche la complessità propria della struttura aziendale o dell'ente in cui il DPO dovrà operare[344].

Al paragrafo 3 viene previsto poi che titolare e responsabile non diano istruzioni al DPO circa l'esecuzione delle sue funzioni e, ulteriormente, si assicurino che questi non riceva alcuna penalizzazione per l'esecuzione degli stessi. È proprio tale previsione a mettere in risalto, con maggiore evidenza, il carattere di indipendenza del ruolo del DPO. Se il requisito di autonomia deriva dalla realizzazione delle condizioni sopra analizzate, vale a dire dalla messa a disposizione, da parte del titolare, di tutti gli strumenti necessari per lo svolgimento proficuo dell'incarico, il requisito dell'indipendenza può intendersi maggiormente pertinente ad una dimensione psicologica e mentale del DPO, che

[344] Sarebbe utile prevedere, nell'ambito della lettera di incarico o del contratto di servizi, che il DPO riferisca periodicamente ai vertici operativi (l'organo amministrativo ma anche quello di controllo), attraverso relazioni trimestrali o semestrali o annuali, non solo in merito all'attività svolta, nonché alle eventuali criticità riscontrate, ma anche facendo un resoconto relativo alla gestione del *budget* che gli viene affidato.

deve mantenersi estraneo ad ogni forma di interferenza, condizionamento o pressione da parte dei vertici aziendali o dell'ente, e non deve trovarsi in una condizione di subalternità rispetto a questi ultimi, ma deve essere gerarchicamente collocato a fianco del vertice della "linea di comando". Secondo il WP29, le caratteristiche di cui sopra si sostanziano, in particolare, nella libertà del DPO di consultare l'Autorità di controllo per averne un parere, di fornire egli stesso i pareri anche quando non interpellato direttamente, e in generale di avere un'autonoma visione riguardo ad un certo problema o all'interpretazione della legge.

Su queste considerazioni, autonomia ed indipendenza potrebbero interpretarsi come le due declinazioni, oggettiva e soggettiva, del rapporto tra DPO e titolare/responsabile, con maggiore attenzione l'una (autonomia) al profilo organizzativo e gestionale "materiale" (nonché alla disponibilità di risorse finanziare per l'attività e l'aggiornamento) e l'altra (indipendenza) al profilo dell'organizzazione e svolgimento dei compiti nella loro dimensione immateriale e relazionale tra le figure interessate.

In considerazione della possibilità offerta al titolare di nominare quale DPO tanto un soggetto che si trovi già alle sue dipendenze quanto un soggetto esterno all'organizzazione, è bene analizzare da vicino come le caratteristiche di indipendenza ed autonomia si sostanzino nelle due differenti ipotesi, ed in particolare quali siano i profili che possano incidere in negativo sulle caratteristiche in questione. Per ragioni di sistematicità, inoltre, nell'approfondimento delle due diverse tipologie di incarico, si metteranno in risalto anche ulteriori profili critici inerenti l'uno e l'altro caso, dovuti in alle lacune presenti dalle previsioni normative e non colmate dal legislatore nazionale.

6.3.1 Il *Data Protection Officer* interno

Nel caso in cui ad essere nominato DPO sia un soggetto già dipendente dell'azienda o dell'ente pubblico, i requisiti di autonomia e indipendenza che dovrebbero caratterizzarne lo *status* potrebbero esser messi in dubbio, stante la possibilità che si configuri un conflitto di interessi in relazione alle altre funzioni

espletate, e ciò soprattutto se, in qualità di DPO, vengano attribuiti al dipendente compiti e funzioni ultronee rispetto a quelle indicate dal GDPR.

Lo stesso art. 38, al paragrafo 6 prende in considerazione tale eventualità, riferendo appunto della possibilità di un conflitto di interessi proprio nell'ipotesi in cui al DPO vengano affidati compiti ulteriori rispetto a quelli indicati nel testo di legge: in tal caso, sarà onere del titolare o del responsabile accertarsi che non si realizzino, concretamente, situazioni di conflitto di interessi né che le stesse siano astrattamente configurabili. Il conflitto di interessi, peraltro, può aversi non solo in considerazione dello svolgimento di mansioni incompatibili tra loro *ratione materiae* (per posizione o per mansione/oggetto del mandato: ad esempio nei casi in cui il DPO sia anche coinvolto nella determinazione delle modalità e finalità del trattamento dei dati) ma, ulteriormente, nei casi di problemi di coordinamento tra il tempo impiegato nell'adempimento delle mansioni di DPO e quello dedicato agli altri compiti svolti in virtù della funzione principale, con il rischio che le mansioni inerenti alla carica di DPO vengano "sopraffatte" dagli adempimenti derivanti dalle altre funzioni[345].

Al fine di evitare che ciò avvenga, il WP29 ha suggerito che i titolari del trattamento individuino previamente, a seconda delle attività, delle dimensioni e della struttura dell'organizzazione, le posizioni interne che potrebbero, potenzialmente, essere incompatibili con la funzione di DPO, e diano conto di tali incompatibilità attraverso l'elaborazione di un apposito regolamento interno (onde evitare altresì eventuali contenziosi). Altresì, il WP29 ha suggerito che il titolare predisponga atti di conferimento di incarico sufficientemente precisi e dettagliati, in modo da essere in grado di dimostrare, in caso di contestazioni da parte di terzi, l'assenza del conflitto di interessi tra le funzioni già espletate dal dipendente e quelle derivanti dall'incarico di DPO.

Nella fase iniziale di assestamento e adeguamento alla nuova normativa europea, alcuni enti avevano incaricato della funzione di DPO quei dipendenti che, svolgendo incarichi dirigenziali, e dunque essendo già in ruoli apicali ed essendo già a conoscenza di ogni aspetto inerente i trattamenti da porre in essere, potevano

[345] G. BUTTI, *Il DPO e il rischio di conflitto di interessi: profili e allocazione delle responsabilità*, 23 aprile 2019, rinvenibile al link *https://www.cybersecurity360.it/legal/privacy-dati-personali/il-dpo-e-il-rischio-di-conflitto-di-interessi-profili-e-allocazione-delle-responsabilita/*.

apparire non solo più competenti a svolgere l'ulteriore incarico di DPO, ma altresì, le figure più idonee da nominare anche perché meno esposti ad eventuali ingerenze datoriali "dall'alto", non trovandosi in posizione di subalternità nei confronti del titolare o del responsabile.

Tuttavia, contrariamente a quanto ci si attendeva, tale intuizione si è rivelata erronea, poiché il confluire di un doppio incarico in capo a soggetti che, nell'ambito dell'organizzazione di riferimento, rivestivano ruoli di carattere dirigenziale, dava spesso luogo a conflitti di interesse, anche solo potenziale, tra ruolo "controllante" e ruolo "controllato"[346].

Alla luce di quanto sopra, si ritiene dunque opportuno , allo stato attuale ed ai fini di una più attenta *compliance* aziendale, escludere dall'incarico di DPO coloro i quali svolgano funzioni di vertice, che concorrono all'individuazione delle finalità e dei mezzi del trattamento, ivi incluse le mansioni più vicine al *core business* aziendale (a titolo esemplificativo l'amministratore delegato, il direttore operativo, il direttore finanziario, la direzione risorse umane, la direzione *marketing*, il responsabile IT, il responsabile ufficio legale e così via).

Potrebbero allora essere nominati DPO i lavoratori che si trovino in una posizione di livello intermedio nel dipartimento e/o ufficio dell'azienda o dell'ente, garantendo loro, nello svolgimento dei compiti di DPO, un canale preferenziale nei confronti dei vertici aziendali/titolare e responsabile, cioè gli unici con i quali si andrebbero a relazionare. Ancora, tali dipendenti potrebbero essere garantiti, nei confronti di eventuali contestazioni strumentali ad incidere sull'operato quali DPO, attraverso la predisposizione di rafforzate misure di tutela sindacali. Difatti,

[346] Un caso particolare si è verificato, ad esempio, in Germania, ove un'azienda aveva assegnato l'incarico di DPO al Responsabile del settore informatico. Il caso in esame è stato oggetto di attenzione da parte dell'Autorità Bavarese (*Bavarian Data Protection Authority - BayLDA*), la quale ha espressamente riconosciuto l'incompatibilità dei due ruoli, comminando una sanzione alla società per aveva nominato il proprio IT manager come DPO. L'Autorità rilevava che, nel caso in esame, non fosse possibile far confluire, in capo al medesimo soggetto, la funzione di controllore e controllato, conseguenza diretta del fatto che il soggetto in questione era al contempo incaricato di predisporre il sistema di sicurezza idoneo ad evitare che il trattamento venisse esposto a rischi e verificare da sé se le attività svolte in qualità di IT manager fossero o meno conformi alla normativa in materia di protezione di dati personali. Tale forma di auto-monitoraggio si è ritenuta, ovviamente, contrastante con la *ratio* del ruolo di DPO, soprattutto con riferimento alla necessità di garantirne l'indipendenza nell'esercizio delle funzioni.Cfr. N. BERNARDI, *Il Garante per la privacy bavarese si prepara a sparare sulla Croce Rossa*, rinvenibile al link *https://nicolabernardi.nova100.ilsole24ore.com/2019/08/31/il-garante-privacy-bavarese-pronto-a-sparare-sulla-croce-rossa/*.

non deve essere tralasciato che, anche in questi casi, il conflitto di interessi si potrebbe generare in considerazione della loro posizione subalterna rispetto ai loro diretti superiori gerarchici, che non consentirebbe loro di "denunciare" eventuali condotte colpose di questi ultimi ai vertici aziendali, pena il rischio di subire delle ricadute in relazione alla loro attività principale. Altresì, qualora i diretti superiori gerarchici dei dipendenti incaricati a DPO siano al contempo proprio i vertici aziendali, bisognerà valutare se effettivamente i dipendenti siano disposti a denunciare loro comportamenti o valutazioni erronee.

In ogni caso, occorre ribadire che il legislatore ha previsto, all'art. 38, par. 3, a maggior sostegno della sua indipendenza, che il DPO non possa essere rimosso o penalizzato dal titolare o dal responsabile del trattamento per l'adempimento dei propri compiti[347]: tale previsione, formulata in modo generico, potrebbe dar luogo a problemi d'interpretazione, soprattutto in considerazione del fatto che la stessa è rivolta non solo al DPO già dipendente, ma anche al DPO esterno. Una tale previsione può interpretarsi, peraltro, come ulteriore sostegno della astrattezza e genericità delle norme in materia, che non pongono in essere un'adeguata distinzione tra DPO di enti pubblici o privati, e ulteriormente tra DPO già dipendenti o esterni. Del resto, entrambi i concetti di penalizzazione e rimozione sopra richiamati possono avere senso solo se riferiti al DPO già dipendente della società o ente, a meno che non si voglia dare spazio a interpretazioni diverse, che sembrano tuttavia fuorvianti.

In relazione a tali problematiche, ciò che si vuole sostenere è che, con riferimento al concetto di "penalizzazione", lo stesso può venire in rilievo sia come rimprovero per il mancato o negligente inadempimento per le funzioni di DPO in sé e per sé considerate, sia (ma solo se il DPO è un soggetto già dipendente) con riferimento alle altre mansioni derivanti dal rapporto di lavoro e svolte in via principale in qualità di dipendente: nel primo caso, il divieto di penalizzare il dipendente per le sue mansioni da DPO, dovrebbe tradursi nella impossibilità per

[347] Esempi di penalizzazione potrebbero essere rintracciati nella mancata o ritardata promozione, nel blocco delle progressioni di carriera, nella mancata concessione di incentivi rispetto ad altri dipendenti. Non è necessario che si arrivi all'effettiva applicazione di una penalizzazione, essendo sufficiente anche la mera minaccia, nella misura in cui sia rivolta al DPO in rapporto alle attività da questi svolte. Cfr. M. IASELLI, *DPO di un ente pubblico: qualifica e requisiti*, rinvenibile al link *https://www.agendadigitale.eu/sicurezza/privacy/dpo-di-un-ente-pubblico-qualifica-e-requisiti*.

il titolare di muovere alcun tipo di rimprovero a questi per il suo operato, mentre, nel secondo caso, nel divieto, per lo stesso titolare, di intraprendere azioni che possano avere ripercussioni sul rapporto di lavoro principale.

Se, in relazione al secondo caso appare oltremodo ragionevole la previsione in esame, al contrario, con riferimento al primo caso, essa appare troppo generica: è improbabile credere che non vi possano essere in concreto situazioni in cui il titolare non possa muovere alcun rimprovero al DPO, ad esempio in tutti quei casi in cui questi non abbia svolto il proprio compito in maniera diligente (solo a titolo esemplificativo, si può citare l'eventuale obbligo di tenuta del registro, conferito espressamente al DPO ma da questi non correttamente adempiuto).

Anche il riferimento alla "rimozione" dall'incarico desta qualche dubbio: se la stessa appare ragionevole in relazione al rapporto di lavoro principale già intercorrente tra il titolare ed il dipendente (poiché è evidente che il dipendente non possa essere rimosso dal suo incarico in virtù delle mansioni svolte in qualità di DPO) appare meno comprensibile il divieto di rimozione rivolto all'incarico di DPO in sé e per sé considerato. È naturale, infatti, attendersi che, in una qualsiasi organizzazione, sia aziendale che pubblica, il soggetto che ha provveduto alla designazione ed abbia instaurato col designato un rapporto di fiducia e collaborazione, possa avere interesse a rimuovere dall'incarico il soggetto che si sia rivelato inidoneo a svolgere i compiti assegnati o che abbia tradito il rapporto di fiducia in questione

Su queste considerazioni sorge un nuovo problema, che coinvolge anche i casi di nomina del DPO esterno, posto che la legge non specifica i casi in cui si può dar luogo a rimozione, potendo così la stessa rimozione rivelarsi illegittima. In particolare, la legge non specifica se la revoca vada disposta esclusivamente per giusta causa oppure se sia ammissibile una revoca *ad nutum*. Pare preferibile la tesi secondo la quale la revoca debba avvenire soltanto al ricorrere della giusta causa, in considerazione della circostanza per cui (come si avrà modo di analizzare più avanti), la prestazione del DPO debba essere ricondotta nel novero delle prestazioni d'opera intellettuale, da ciò derivando il risarcimento del danno a favore di quest'ultimo in caso di rimozione senza giusta causa.

Con riferimento al caso in esame, tuttavia, è opportuno chiedersi cosa debba intendersi per "giusta causa": la delicatezza dell'argomento avrebbe forse reso preferibile un intervento più incisivo del legislatore, soprattutto in considerazione del fatto che, qualora il DPO decida di contestare la decisione da parte del titolare, è ragionevole ipotizzare che tale scelta possa altresì incidere negativamente sul rapporto di lavoro principale.

Solo a titolo esemplificativo, potremmo ipotizzare che la giusta causa si configuri non solo in tutte quelle ipotesi in cui il DPO svolga in maniera negligente le sue funzioni, ma anche per altre ragioni più particolari, ad esempio nel caso in cui il titolare sia stato destinatario di numerose sanzioni per il mancato rispetto delle norme e degli obblighi ex GDPR, e ciò possa essere ricondotto alle valutazioni ed all'operato dal DPO. Ancora, proprio nello specifico caso del dipendente interno nominato DPO, si potrebbe ipotizzare sussistere la giusta causa nel caso della eventuale risoluzione del rapporto principale.

Tuttavia, come si diceva, la legge è oltremodo vaga con riferimento ai concetti di penalizzazione e rimozione e, soprattutto, non opera alcuna distinzione tra DPO interno o esterno. Si ritiene, in ogni caso, di aderire alla tesi secondo la quale penalizzazione e revoca vadano riferite esclusivamente al soggetto già dipendente dell'organizzazione, e siano riferite, e dunque vietate, rispetto alle funzioni da questi svolte in via principale, lasciando così aperta la possibilità per il titolare di penalizzare o revocare il DPO per l'inadempimento dei compiti svolti in ragione di tale ruolo.

È chiaro, inoltre, che, anche in considerazione della necessità di salvaguardia del carattere di indipendenza, sarebbe forse stato auspicabile, da parte del legislatore, prevedere un ruolo più incisivo dell'Autorità di controllo, nel caso in cui si verifichi un'ipotesi di penalizzazione o revoca del DPO, e ciò sia con riferimento al dipendente interno (a maggior ragione poi nelle ipotesi in cui il DPO lavori alle dipendenze di un ente pubblico), sia con riferimento all'incaricato esterno. Si potrebbe fare riferimento, in tal senso, a quanto già previsto dal Regolamento 2001/45/CE relativo al trattamento dei dati personali posti in essere dalle istituzioni e organismi comunitari. Ai sensi dell'art. 24, n. 4, come si è visto, viene sancito che, nel caso in cui l'istituzione voglia destituire il DPO perché questi non

soddisfa più le condizioni richieste per l'esercizio delle sue funzioni, è necessario che vi sia il previo consenso del Garante europeo. Introdurre la possibilità di una previa consultazione dell'Autorità di controllo potrebbe essere un buon meccanismo per garantire al DPO la possibilità di agire senza aver paura di subire ritorsioni che possano rivelarsi illecite. Tale possibilità, inoltre, era già prevista nell'ordinamento tedesco, ove può individuarsi anzi una disposizione che prevede la possibilità per l'Autorità stessa di segnalare al titolare l'opportunità di una rimozione.

Ma l'Autorità Garante potrebbe essere chiamata a intervenire anche, ad esempio, nel caso in cui vi sia il dubbio che il titolare abbia proceduto a una penalizzazione del DPO con riferimento all'incarico principale svolto in qualità di dipendente.

Tale possibilità, del resto, non è del tutto nuova nel nostro panorama nazionale. Si vuol fare riferimento, al riguardo, alla materia dell'anticorruzione, la cui disciplina è contenuta nella legge 6 novembre 2012, n. 190, anche nota come "legge Severino" o "legge anticorruzione", emanata al fine di contrastare il pervasivo fenomeno della corruzione nel settore pubblico. Il sistema delineato da tale legge si caratterizza, esattamente come avviene in quello di protezione dei dati personali, per l'impronta di carattere preventivo della tutela predisposta, che si affianca al tradizionale approccio repressivo che connotava il sistema italiano, che però iniziava a mostrare i propri limiti[348]. La legge in esame introduce una serie di nuovi organismi pubblici a presidio del sistema costruito, quali, tra gli altri, l'Autorità Nazionale Anti Corruzione (ANAC), nonché organi interni alle singole amministrazioni, vale a dire il Responsabile della prevenzione della corruzione (RPCT), anche noto come Responsabile anticorruzione.

Il RPCT, sul quale si tornerà altresì nel successivo capitolo, è una figura interna alle amministrazioni (trattandosi di una persona già alle dipendenze delle stesse) che, sotto molti punti di vista, presenta diversi punti di contatto con la figura professionale del DPO interno. Tuttavia, ciò che contraddistingue profondamente le due figure è il rapporto che le lega alle Autorità pubbliche poste a presidio della tutela del settore di riferimento, posto che il rapporto tra RPCT e ANAC ha delle

[348] R. CANTONE – E. CARLONI, *La prevenzione della corruzione e la sua Autorità*, in *Diritto pubblico*, 3/2017, Il Mulino, pp. 94-95.

ricadute notevoli sul rapporto che intercorre tra RPCT e ente in cui lo stesso opera.

In particolare, per quanto di interesse ai fini della presente indagine, la legge anticorruzione prevede, all'art. 1. c. 7 che eventuali misure discriminatorie, dirette o indirette, nei confronti del RPCT per motivi collegati, direttamente o indirettamente, allo svolgimento delle sue funzioni, devono essere segnalate all'ANAC, che può chiedere informazioni all'organo di indirizzo e intervenire formulando un parere di riesame del provvedimento, qualora appunto rilevi che lo stesso sia correlato alle attività svolte dal RPCT. In sostanza, viene previsto un sistema ampio di tutela e garanzia del RPCT, che prevede l'intervento dell'ANAC su misure discriminatorie anche diverse dalla revoca, perpetuate nei confronti di quest'ultimo per motivi collegati, direttamente o indirettamente, allo svolgimento delle sue funzioni.

Le considerazioni svolte mirano a stimolare una riflessione circa, appunto, la possibilità di una revisione di questo particolare aspetto della disciplina, inerente il rapporto tra Autorità e DPO, anche al fine di poter garantire al dipendente una tutela migliore e, indubbiamente, una maggiore indipendenza nello svolgimento del proprio incarico. Come si vedrà, inoltre, la modifica di tale rapporto può essere giustificata anche alla luce di altri fattori che verranno meglio analizzati nel prosieguo.

Allo stato dell'arte, stante l'attuale assenza di una indicazione normativa in tal senso, e proprio in ragione di questa lacuna, sarebbe opportuno per il titolare stabilire nella lettera di incarico, con un grado di precisione elevato, i casi e le condotte che potrebbero dar luogo alla penalizzazione o alla revoca dell'incarico.

Alla luce delle considerazioni svolte in merito alla nomina della persona fisica già dipendente dell'ente, pare forse più opportuno per il titolare del trattamento nominare quale DPO un soggetto esterno "per scongiurare ogni eventuale deriva centripeta e distorsiva dell'azione del DPO interno"[349].

[349] R. PANETTA, *DPO interno o esterno? Ecco dove si nasconde il conflitto di interessi*, rinvenibile al link *https://www.agendadigitale.eu/sicurezza/privacy/dpo-interno-o-esterno-ecco-dove-si-nasconde-il-conflitto-di-interessi/*.

6.3.2 Il *Data Protection Officer* esterno

La scelta di incaricare quale DPO un soggetto esterno alla realtà in cui questi andrà ad operare appare essere la migliore in relazione alla necessità di salvaguardare l'indipendenza del ruolo in esame. Un soggetto esterno alla società non avrebbe infatti alcun problema a relazionarsi con qualsiasi figura dell'ente o dell'azienda e non avrebbe alcun condizionamento determinato dai possibili riflessi positivi/negativi sui rapporti di lavoro già in essere (né in termini di aspirazioni ad eventuali promozioni interne né in termini di timore per sanzioni e/o demansionamento).

Tuttavia, ciò non significa che il conflitto di interesse non possa sorgere in relazione ad altri fattori, legati comunque ad una visione distorta, quali ad esempio il mantenimento dell'incarico o la ricerca di ulteriori benefit o vantaggi dal titolare. Ad esempio, il consulente esterno nominato DPO potrebbe avere interesse ad essere riconfermato nell'incarico, e quindi a non perdere la consulenza: questo potrebbe indurlo ad un atteggiamento di condiscendenza nei confronti del titolare, anche a scapito della tutela degli interessati, poiché potrebbe non indicare al titolare possibili correzioni inerenti attività maggiormente rischiose o addirittura poste in essere in violazione/mancata considerazione dei principi del GDPR.

Al fine di prevenire tale deriva, una eventuale soluzione potrebbe essere offerta dalla possibilità di prevedere incarichi dalla durata predeterminata: ciò consentirebbe non solo al DPO di poter svolgere le proprie attività con maggior serenità e una miglior capacità di programmazione ma, di conseguenza, al titolare, di strutturare i processi di controllo e gestione in materia di protezione dei dati personali con una maggior lungimiranza e coerenza nel corso del tempo, riducendo così il rischio di conflitto di interessi del DPO[350].

Ma il conflitto di interessi potrebbe altresì insorgere allorquando il DPO esterno non dedichi sufficienti risorse all'incarico perché, ad esempio, ha

[350] Nella proposta di regolamento del 2012, all'art. 35 comma 7 era stato previsto che "i*l titolare del trattamento o il responsabile del trattamento designa un responsabile della protezione dei dati per un periodo di almeno due anni. Il mandato del responsabile della protezione dei dati è rinnovabile. […]*": da tale previsione si evince come la volontà del legislatore europeo fosse quella di garantire una maggior indipendenza del ruolo di DPO attraverso la previsione di una durata minima biennale dell'incarico.

cumulato incarichi per diversi titolari, che si rivelano poi eccessivi per le risorse a sua disposizione. Ancora, potrebbe verificarsi un conflitto di interessi in tutti quei casi in cui l'incarico di DPO venga affidato ai consulenti che abbiano assistito il titolare o il responsabile nel percorso di adeguamento al GDPR: l'incompatibilità dei ruoli è oltremodo evidente, in quanto il DPO dovrebbe verificare e intervenire su un sistema di gestione del trattamento dei dati personali alla cui realizzazione egli stesso ha partecipato[351].

Aldilà del caso in cui si verifichino le ipotesi summenzionate, tuttavia, la nomina di un soggetto esterno sembra potersi considerare la scelta migliore, proprio in considerazione della maggiore possibilità per il DPO di essere realmente indipendente ed autonomo rispetto al titolare.

Altresì non deve sottovalutarsi l'opportunità, per il titolare, di affidarsi a soggetti che abbiano maturato un'esperienza notevole e variegata nel settore di riferimento, specie nel caso in cui l'incarico venga affidato non ad una persona fisica ma ad una persona giuridica, quindi ad una società composta da più professionisti, che compendi profili professionali specializzati in ambito legale ed altri specializzati in ambito tecnico.

In caso d nomina della persona giuridica, tuttavia, deve evidenziarsi come sia pur sempre essenziale che la stessa indichi quale soggetto fisico sarà espressamente incaricato a rivestire il ruolo di DPO per il titolare ed assumere le relative funzioni ed obblighi. L'individuazione del soggetto DPO è necessaria poiché, sebbene sia chiaro che questi potrà avvalersi dell'ausilio da parte degli altri dipendenti della società, non sarà, invece, ammissibile che le funzioni vengano affidate ad una pluralità di dipendenti della società nominata, né potrà essere ammissibile introdurre un principio di rotazione in virtù del quale i soggetti incaricati a svolgere la funzione di DPO presso quello specifico titolare potranno variare al ricorrere di determinate circostanze.

Del resto, il fattore umano, la consuetudine, la conoscenza delle altre funzioni aziendali, degli strumenti *software* dell'azienda, dell'insieme dei mezzi e dei fini del trattamento – senza mai contribuire alla loro determinazione – fanno la differenza e rendono il rapporto tra titolare e persona fisica componente della

[351] R. PANETTA, op. cit.

società incaricata un rapporto personale, sebbene il contratto sia stipulato, appunto, tra titolare e società incaricata[352].

È chiaro, tuttavia, che la nomina di una società solleva più di un dubbio di carattere interpretativo, che potrebbe avere delle ripercussioni in punto di responsabilità, sia con riferimento alla società incaricata nei confronti del titolare, sia con riferimento alla persona fisica indicata quale punto di contatto tra titolare e società nei confronti di quest'ultima. Posto, infatti, che i rapporti tra titolare e società devono essere regolati dal contratto di servizi cui fa riferimento il GDPR, nulla viene indicato con riferimento alla designazione del soggetto ed alla regolazione dei rapporti tra titolare e persona fisica indicata quale incaricato effettivo della società, sicché il rapporto di preposizione (sul quale, altresì, si incentrano i dubbi su una possibile inferenza del titolare) verrebbe a costituire l'unica base giuridica di riferimento per identificare il regime dei ruoli e delle responsabilità. Diversamente, dovrebbe ipotizzarsi una regolazione contenuta in un formale atto di preposizione (da parte della società) in relazione al quale, tuttavia, non appare chiaro quale potrebbe essere, almeno in fase di formazione, il ruolo del titolare.

Sono tanti, e di varia natura, i problemi che potrebbero sorgere in questi casi, fatto salvo quanto già specificato con riferimento al DPO interno, in merito alle ipotesi di penalizzazione o revoca, posto che si tratta di considerazioni estensibili anche al DPO esterno.

Ad esempio, si pensi all'ipotesi in cui dovesse venir meno il rapporto tra la società incaricata ed il suo dipendente: la cessazione di questo rapporto andrà ovviamente a incidere sul diverso rapporto instaurato tra titolare e persona fisica indicata. Potrebbe, infatti, accadere che il titolare sia interessato a mantenere il rapporto con il soggetto designato dalla società per svolgere l'incarico. Cosa accadrà in tal caso? È lecito ammettere la possibilità per il titolare di recedere dal contratto con la società? E, ulteriormente, è ammissibile che il titolare chieda un risarcimento?

Ancora, si pensi al caso in cui la persona fisica indicata dalla società sia inadempiente nei confronti del Titolare. In tal caso, il Titolare presumibilmente vorrà sciogliere il contratto stipulato con la società od addirittura, in caso di

[352] R. PANETTA, op. cit.

danno, avanzare pretese risarcitorie. Quest'ultima, al ricorrere dell'ipotesi passata in rassegna, potrà rivalersi sul dipendente, ma potrà ciò costituire anche una eventuale ipotesi di licenziamento per giusta causa?

Le situazioni così tratteggiate costituiscono solo alcune delle circostanze che possono venire in rilievo nell'ambito dei rapporti tra titolare, società data protection e soggetto designato quale DPO; in tutti questi casi, sarà sicuramente necessario definire in via preventiva, sia nel contratto di servizi tra titolare e società incaricata, quanto nell'atto di preposizione/designazione tra quest'ultima e il suo dipendente, quali condotte adottare e quali conseguenze collegare alle ipotesi evidenziate.

6.3.2.1 La sentenza del TAR Lecce del 13 settembre 2019, n. 1468

Con specifico riferimento alla nomina di una società esterna, merita di essere segnalata la recente sentenza del TAR Lecce del 13 settembre 2019, n. 1468[353], con la quale è stato sancito che, se l'incarico di DPO è assegnato ad una società esterna, la persona fisica che agisce per suo conto nei rapporti con il titolare, deve necessariamente appartenere all'organico della persona giuridica assegnataria.

La pronuncia, pur occupandosi della nomina del DPO nel settore pubblico (si tratta infatti di un caso relativo ad assegnazione dell'incarico di DPO da parte di un Comune), sancisce un principio che si presta a trovare applicazione anche in ambito privatistico.

In particolare, nella vicenda in questione, il TAR ha annullato l'aggiudicazione, da parte di una società a responsabilità limitata, di un incarico biennale di DPO affidatole da un Comune, poiché la stessa aveva indicato quale incaricato allo svolgimento dell'attività un consulente esterno alla medesima.

La motivazione adottata dal Giudice amministrativo si basa sulla considerazione che l'ufficio di DPO non possa essere affidato ad una persona esterna alla società affidataria dell'incarico, ma necessariamente ad una persona "appartenente" alla struttura o all'organico della stessa.

Il Giudice, richiamando la versione italiana delle linee guida del WP29, considerate dallo stesso giudicante testo d'interpretazione autentica del GDPR,

[353] Sentenza TAR Puglia, Lecce, sez. III, 13/9/2019 n. 1468.

nella parte in cui specificano che "è indispensabile che ciascun soggetto appartenente alla persona giuridica e operante come R.P.D. soddisfi tutti i requisiti applicabili come fissati nella sezione 4 del RGPD", evidenzia come tali linee guida richiedano, implicitamente, ma inequivocabilmente, che la persona fisica operante come DPO debba essere "appartenente" alla persona giuridica, e che tale requisito di "appartenenza" vada provato con documenti contrattuali significativi e coerenti.

Nel caso di specie, secondo la pronuncia del TAR, tale prova di "appartenenza" sarebbe mancata: la mera proposta di incarico allegata in atti dalla società, infatti, non poteva essere considerata idonea a provare il rapporto sotteso tra questa e il soggetto indicato per lo svolgimento dell'attività di DPO, per due ordini di ragioni. La prima valutazione era relativa alla circostanza per cui la predetta proposta di incarico, datata 12 ottobre 2018, non era stata registrata né allegata alla domanda di partecipazione alla selezione (versata in atti dal Comune di Taranto), da ciò derivando l'impossibilità di dare piena prova del fatto che tra il consulente incaricato quale DPO del Comune e la società affidataria intercorresse un vincolo giuridico preliminare alla partecipazione di quest'ultima alla gara pubblica, come, invero, sostenuto dalla società stessa.

La seconda ragione risiedeva invece nella circostanza per cui «la scrittura privata fra la Isform & Consulting ed il Dr. F.M. del 12 ottobre 2018 parla esplicitamente di un "incarico professionale", ossia di un rapporto non di subordinazione e rientrante nell'alveo delle prestazioni professionali, in cui il soggetto incaricato, ossia il Dr. M., può godere, ai sensi degli articoli 2222 e seguenti del codice civile, di una propria autonomia nell'esplicazione dell'incarico, atteso che la lettera di conferimento non esclude tale possibilità con vincolo contrattuale, così ponendo seri dubbi circa la sussistenza del sopra menzionato requisito dell'appartenenza».

Dunque, secondo il giudice, la "autonomia nell'esplicazione del mandato", implicita nel conferimento d'incarico da parte della società nei confronti dell'incaricato, sarebbe incompatibile con quanto richiesto dal GDPR. Così ragionando, il giudice assimila il concetto di appartenenza a quello di dipendenza/subordinazione, da ciò deducendo che il ruolo di DPO non possa

essere svolto da una figura che non sia sottoposta a un vincolo di subordinazione nei confronti della persona giuridica cui viene affidato l'incarico da parte del titolare. Di talché, posto che dalla lettera d'incarico dedotta in atti risaltava la connotazione autonoma dell'incarico affidato dalla società alla persona fisica, e che l'autonomia è il requisito tipico caratterizzante la libera professione, la nomina andava ritenuta illegittima.

L'interpretazione offerta, tuttavia, non sembra del tutto condivisibile, dal momento che, probabilmente, sarebbe stato più opportuno interpretare tale concetto di "appartenenza" come necessità di un coinvolgimento del lavoratore nella società, che non deve necessariamente manifestarsi nelle forme di una subordinazione al datore di lavoro, tipico del rapporto di lavoro dipendente[354]. D'altronde, appare piuttosto illogico sostenere che la persona fisica, che svolge l'incarico di DPO, debba essere indipendente ed autonoma rispetto al titolare del trattamento, ma al contempo obbedire agli ordini dell'ente incaricato a svolgere il ruolo del DPO.

Secondo alcuni commentatori, inoltre, la questione di vero rilievo sarebbe quella relativa alla qualificazione del contratto intercorrente tra la società ed il soggetto da questa incaricato come DPO. In particolare, ci si è chiesti se tale contratto possa essere ricompreso in quello di subappalto disciplinato ex art. 105 D. Lgs. 50/2016 (sebbene il comma 2 escludi dal novero del subappalto l'affidamento di attività specifiche a lavoratori autonomi, per le quali occorre effettuare comunicazione alla stazione appaltante, e le prestazioni rese in favore dei soggetti affidatari in forza di contratti continuativi di cooperazione, servizio e/o fornitura sottoscritti in epoca anteriore alla indizione della procedura finalizzata alla aggiudicazione dell'appalto), o se sia utilizzabile l'istituto dell'avvalimento, di cui all'art. 89 del Codice degli Appalti[355]. Sul punto, si consideri che il codice prevede espressamente che l'appaltatore possa avvalersi di soggetti terzi per l'espletamento dell'opera o del servizio affidatogli dalla PA, imponendo soltanto che il contratto di avvalimento sia preesistente alla domanda di partecipazione alla

[354] A. CICCIA MESSINA, *Stop all'incetta di nomine di data protection officer*, rinvenibile al link *https://federprivacy.org/informazione/primo-piano/item/1029-dpo-stop-alla-incetta-di-nomine.*

[355] Cfr. G. B. GALLUS, *Il DPO deve essere dipendente dell'azienda affidataria dell'incarico": il Tar Lecce fa discutere*, reperibile al link *https://www.cybersecurity360.it/news/il-dpo-deve-essere-un-dipendente-non-puo-essere-esterno-il-tar-lecce-fa-discutere/*.

gara e abbia una data certa antecedente alla presentazione della candidatura: nel contratto di avvalimento, peraltro, è pacifico che l'ausiliario non è "dipendente" del concorrente in gara.

Accanto alle considerazioni sin qui svolte, merita di essere messa in luce un'ulteriore riflessione: il giudice, nel decidere il caso in esame, interpreta la versione italiana delle Linee guida, e non la versione ufficiale redatta in lingua inglese. Dal confronto delle due, emerge che la versione inglese si limita a specificare che tutti i membri della persona giuridica (team) nominata DPO debbano soddisfare i requisiti previsti dal GDPR e che agli stessi vengano riconosciute le relative garanzie, senza imporre loro alcun rapporto di dipendenza o para-subordinazione rispetto alla società[356]. Pertanto, se il giudice si fosse attenuto alla versione inglese delle Linee guida (che è poi quella ufficiale) non è difficile ipotizzare che sarebbe giunto ad una diversa conclusione, cioè che, allorquando l'incarico sia affidato ad una persona giuridica, e non ad una fisica, questo possa essere svolto da chiunque sia legato alla persona giuridica da un rapporto di lavoro subordinato ovvero da un contratto d'opera intellettuale.

6.3.3 La composizione collegiale dell'ufficio del *Data Protection Officer*: prospettive e vantaggi

Le diverse considerazioni svolte nei precedenti paragrafi, sia in merito alla necessità che il DPO disponga di diverse conoscenze e competenze per poter svolgere adeguatamente l'incarico (conoscenze e competenze che, come si è visto, devono essere principalmente di carattere giuridico, ma senza tralasciare quelle di natura tecnica), sia quelle relative alla necessità che al DPO vengano garantite autonomia d'azione ed indipendenza nei confronti del titolare o del responsabile, consentono di poter proporre, quale migliore soluzione per ottenere il risultato atteso, la costituzione di un vero e proprio ufficio, di cui il DPO andrebbe a

[356] È stato altresì evidenziato che "*è singolare che il TAR non consideri in alcun modo il dettato normativo primario (gli artt. 37 e ss del GDPR, e il relativo Considerando 97), ma si concentri esclusivamente sulle Linee guida, che vengono addirittura elevate a "interpretazione autentica" (così, testualmente, nella sentenza) della normativa europea*". Infatti, le Linee guida non hanno alcuna valenza precettiva "*essendo espressione tipica di soft law, utile per l'interprete, ma non certo cogente*". Cfr. G. B. GALLUS, op. cit., reperibile al link *https://www.cybersecurity360.it/news/il-dpo-deve-essere-un-dipendente-non-puo-essere-esterno-il-tar-lecce-fa-discutere/*.

rappresentare il vertice operativo. Nulla vieta, come si è visto, che venga nominato un *team* di persone, potendo far ricorso alla nomina di una società esterna, sebbene sia necessario, in tal caso, che uno solo dei dipendenti della società sia indicato come punto di contatto con il titolare. Inoltre, stante la constatazione per cui il ricorso a una composizione collegiale sia da privilegiare, piuttosto che ricorrere direttamente a una società esterna, si potrebbe nominare quale DPO una persona fisica esterna (che sarebbe in grado di garantire i requisiti di autonomia ed indipendenza), che andrebbe a lavorare con un *team* composto da soggetti interni e predisposto dal titolare (in grado di assicurare, da un lato, approfondita conoscenza dei profili organizzativi e gestionali dell'Ente, dall'altro lato la continuità d'azione richiesta dalla norma e dalla prassi).

7. Le funzioni del *Data Protection Officer*

L'articolo 39 del GDPR contiene un elenco dei compiti tipici di cui deve farsi carico il DPO, che, con indicazione volutamente generica, deve occuparsi "almeno" dei seguenti compiti:

a) informare e fornire consulenza al Titolare o il Responsabile del trattamento, nonché ai dipendenti dell'organizzazione di appartenenza che eseguono il trattamento, in merito agli obblighi derivanti dal Regolamento europeo e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati (tale necessità si spiega in particolar modo per i casi in cui il Titolare ponga in essere trattamenti transfrontalieri di dati);

b) verificare l'attuazione e l'applicazione del Regolamento, delle altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare o del Responsabile del trattamento in materia di protezione dei dati personali, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento e alle connesse attività di controllo (i c.d. audit);

c) fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne il corretto svolgimento ai sensi dell'art. 35 GDPR;

d) cooperare con il Garante per la protezione dei dati personali;

e) fungere da punto di contatto per l'Autorità di controllo in merito a qualunque problematica connessa al trattamento dei dati o all'esercizio dei diritti da parte degli interessati al trattamento (in sostanza, garantire agli interessati la possibilità di esercitare i propri diritti rivolgendosi ad un soggetto competente senza la necessità di dover ricorrere al Garante per la protezione dei dati).

È interessante porre l'attenzione sulla formulazione della parte introduttiva della norma: dall'avverbio "almeno" utilizzato dal legislatore prima di procedere all'elencazione dei compiti è possibile dedurre che il DPO, oltre ai compiti indicati nelle lettere da a) ad e), possa svolgere anche ulteriori compiti assegnati dal titolare o dal responsabile del trattamento, che devono risultare dalla lettera di incarico ovvero dal contratto di servizi cui fa riferimento l'art. 37 GDPR. Naturalmente, è necessario che i compiti ultronei siano compatibili con quelli elencati dall'art. 39 e, in particolare, non siano tali da determinare situazioni di conflitto d'interessi o compromettere l'indipendenza del DPO, per le ragioni già esposte in precedenza. Infatti, anche rispetto a tali ulteriori funzioni, trova applicazione l'art. 38 par. 3, ove viene stabilito che il titolare ed il responsabile non devono dare alcuna istruzione al DPO per quanto concerne l'esecuzione degli stessi.

Dal disposto dell'art. 39 del Regolamento emerge, con evidenza, non soltanto la molteplicità di compiti cui il DPO è tenuto ad adempiere, che peraltro non si esauriscono in quelli elencati dal legislatore europeo, ben potendo esserne individuati ulteriori, ma altresì emerge la varietà degli stessi, i quali, per sistematicità, possono essere ricondotti a tre categorie principali[357].

In virtù delle sue funzioni consultive, il DPO dovrà offrire assistenza al titolare e al responsabile, e tale assistenza dovrà avere non solo carattere giuridico, ma altresì tecnico, al fine di consentire a questi ultimi di svolgere un trattamento conforme ai princìpi normativi. Da ciò ne deriva che il DPO sarà tenuto ad adempiere, da un lato, a tutti gli obblighi informativi di carattere legale in merito alla normativa nazionale e sovranazionale di protezione dei dati personali che trova applicazione nella realtà di riferimento, e, dall'altro, che questi dovrà svolgere una vera e propria attività di carattere proattivo, vale a dire di

[357] Cfr. C. SOLINAS, *op. cit.*

collaborazione attiva con il titolare e il responsabile, ai fini dell'individuazione dei rischi e delle misure di sicurezza idonee ed adeguate a limitare gli stessi. In tali attività di consulenza rientra altresì l'obbligo di fornire, quando richiesto, un parere (consultivo non vincolante) con riferimento alla valutazione d'impatto sulla protezione dei dati, che è un obbligo di particolare rilievo, per le ragioni che andranno analizzate nel prosieguo.

Con riferimento, invece, alle funzioni di vigilanza e controllo, queste mirano a garantire che il DPO sorvegli in maniera concreta l'osservanza delle norme da parte del titolare, specie con riferimento alle politiche che questi scelga di adottare all'interno della propria organizzazione. L'attività di sorveglianza si estende, peraltro, non solo all'operato del titolare, ma anche a quello dei dipendenti dell'organizzazione, e richiede, in tal senso, che le mansioni di tutti i soggetti che a vario titolo intervengono o sono coinvolti nel trattamento vengano individuate con sufficiente precisione e vengano rese note al DPO, se non siano state direttamente assegnate da lui.

Tale funzione di sorveglianza è particolarmente importante soprattutto nell'ambito dello svolgimento della valutazione d'impatto, che deve essere supervisionata dal DPO: quest'ultimo, infatti, anche nel caso in cui non venga richiesto un parere, potrà in ogni caso rilasciarlo; tale potere deriva proprio dall'obbligo di sorveglianza di cui sopra, rientrando espressamente negli obblighi del DPO indicare al titolare quale sia la condotta migliore da porre in essere nel caso in cui questi non stia operando in modo conforme al GDPR.

Da ultimo, vi è la funzione di cooperazione con l'Autorità, che sarà oggetto di più ampia considerazione nel prosieguo della trattazione, poiché la stessa sembra avere una incidenza di non poco rilievo sulla natura del ruolo in esame, confermandone il carattere, che si sostiene essere "ibrido".

La molteplicità e varietà dei compiti affidati a questa figura determina la difficoltà di individuare una categoria professionale specifica, tra quelle appartenenti al sistema dei controlli interni tipici delle società e degli enti pubblici nell'ambito del nostro ordinamento nazionale, entro cui poter ricondurre la stessa. Il DPO, infatti, inserendosi all'interno del complessivo sistema dei controlli interni proprio non soltanto delle società private ma, ulteriormente, degli enti appartenenti al settore

pubblico[358], e pur presentando delle similitudini con altre figure già note nel nostro ordinamento, specie nell'ambito del diritto societario[359], non può essere assimilato in tutto e per tutto a nessuna di queste, presentando delle peculiarità sue proprie.

In particolare, sebbene le funzioni di consulenza e vigilanza lo rendano per certi versi assimilabile alla nota figura dell'Organismo di Vigilanza, istituito ai sensi del D. Lgs. 231/2001, con cui condivide i medesimi paradigmi strutturali, tuttavia, la posizione di garanzia che questi sembra rivestire nei confronti degli interessati, essendo la sua presenza prevista come obbligatoria in tutti quei casi in cui il loro diritto alla protezione dei dati personali sia esposto a rischi di particolare rilievo (al contrario dell'OdV che, come si vedrà, non è obbligatorio né viene istituito per tutelare interessi terzi, quanto per far andare esente l'ente da eventuali

[358] Il sistema dei controlli interni in ambito societario è uno dei settori più attenzionati da parte del legislatore negli ultimi anni. Questi ha ridefinito le regole che ne determinano il funzionamento, facendo dell'approccio *risk based* il perno della disciplina normativa. La gestione dei rischi aziendali (o *risk management*) costituisce, infatti, uno strumento fondamentale e strategico della *governance* aziendale e societaria, nei suoi molteplici aspetti gestionali, organizzativi e strategici. Il sistema di controllo interno si articola generalmente su tre livelli. Riprendendo le definizioni del Codice di Autodisciplina di Borsa Italiana, al più basso di tali livelli si pongono i controlli c.d. "di linea", che vengono effettuati dal responsabile delle strutture operative interessate, oppure incorporati all'interno delle varie procedure aziendali o svolti nell'ambito dell'attività di *back-office*; ad un grado superiore si trovano i controlli di "secondo livello", tendenzialmente indiretti, poiché basati sui flussi informativi generati dall'operatività a livello inferiore: essi sono affidati a funzioni interne, gerarchicamente sovraordinate, che devono verificare il livello di *compliance*, cioè di conformità alle procedure e alle normative interne ed esterne in materia, effettuando un'attività di *risk management* in senso proprio, cioè di gestione del rischio, idonea non solo a prevenire la commissione di violazioni o il prodursi di eventi avversi, ma anche a fornire opportune indicazioni di indirizzo strategico. Al terzo livello, infine, si colloca, in posizione indipendente all'interno dell'organigramma aziendale e in collegamento immediato con gli organi di vertice a cui riporta direttamente, la funzione c.d. di *internal audit*, che si occupa della revisione generale della struttura e della funzionalità dei controlli interni, nonché dell'individuazione di andamenti anomali, violazioni delle procedure e della regolamentazione, svolgendo così un'attività di prevenzione generale dei rischi e altresì una funzione di consulenza in materia. Al vertice dei sistemi di controllo endosocietari si colloca, poi, in posizione di supremazia, il collegio sindacale, organo istituzionalmente deputato a verificare la diligenza e la conformità alla disciplina legislativa e statutaria dell'operato degli amministratori. V. BANCA D'ITALIA, circolare n. 229/1999, Istruzioni di vigilanza per le banche, Tit. IV, Cap. 11, Sez. II. Cfr. G. GASPARRI, *I controlli interni nelle società quotate. Gli assetti della disciplina italiana e i problemi aperti*, in *Quaderni giuridici*, 4 settembre 2013.
Ed è proprio nell'ambito di questo scenario che si colloca il DPO, che ha come scopo l'assorbimento di uno specifico tipo di rischio, vale a dire quello che il trattamento sia svolto nel rispetto dei princìpi sanciti *ex lege*.

[359] Si pensi, a titolo esemplificativo, al Responsabile del Servizio di Prevenzione e Protezione Aziendale (anche noto come RSPP), figura emblematica nel sistema di gestione della sicurezza del lavoro previsto dal D. Lgs. 9 aprile 2008, n. 81 (c.d. Testo Unico sulla Salute e Sicurezza sul Lavoro), designato dal datore di lavoro al fine di gestire e coordinare le attività del Servizio di Prevenzione e Protezione dai rischi negli ambienti aziendali (SSP).

responsabilità), nonché l'obbligo di cooperazione nei confronti dell'Autorità previsto *ex lege*, richiedono un'indagine più approfondita, al fine di meglio cogliere non solo il portato di tali caratteristiche, ma anche gli eventuali riflessi in punto di natura del ruolo e di responsabilità dello stesso.

Soprattutto, anche allorquando si volesse sostenere il rilievo meramente endo-societario di tale figura nell'ambito dell'azienda o ente in cui essa opera, ritenendo che il principale interesse che la stessa è tenuta a tutelare sia quello del titolare ad essere *accountable* rispetto alla legge, in tal modo garantendo di riflesso anche la tutela del diritto alla protezione dei dati degli interessati, l'obbligo di cooperazione sancito dall'art. 39, lett. d) lascia comunque spazio a interrogativi di non facile risoluzione. Tale obbligo, infatti, interpretato nel senso che meglio si approfondirà, sembra poter richiamare, seppur con le dovute precauzioni, la figura del responsabile della prevenzione della corruzione e della trasparenza (RPCT), istituita dalla legge 6 novembre 2012, n. 190, che ricopre un ruolo di rilievo nella realtà in cui opera, presentandosi come braccio destro dell'Autorità nazionale anticorruzione (ANAC), che è un'Autorità rientrante tra i soggetti pubblici, al pari del Garante per la protezione dei dati personali.

Nel prossimo capitolo, pertanto, dopo aver passato in rassegna le somiglianze e le divergenze rispetto alle richiamate figure dell'OdV e del RPCT, si analizzeranno più da vicino alcuni aspetti che contraddistinguono in modo evidente il DPO dai citati organismi, rendendo lo stesso una figura dotata delle proprie caratteristiche peculiarità, che forse richiederebbero, come si avrà modo di argomentare, un ripensamento di alcuni punti della disciplina, al fine di rendere la figura più funzionale al fine per il quale sembra essere stata pensata.

CAPITOLO QUARTO
IL RUOLO "IBRIDO" DEL *DATA PROTECTION OFFICER*: RILIEVI CRITICI E PROPOSTE *DE IURE CONDENDO*

1. Brevi cenni introduttivi

L'analisi della disciplina del GDPR relativa al DPO ha messo in luce alcune criticità in merito ad una precisa ed esaustiva definizione del ruolo e delle funzioni che la nuova figura professionale potrebbe essere chiamata ad espletare nell'ambito dell'organizzazione aziendale o dell'ente pubblico presso il quale viene designato, nonché nel rapporto con altri soggetti, pubblici e privati.

Se, ad una prima lettura delle norme, potrebbe sembrare che tale figura si connoti per una natura di tipo prettamente privatistico, dati gli interessi e i compiti assegnati, in quanto soggetto, interno o esterno all'organizzazione di riferimento "contrattualizzato" per svolgere determinate funzioni, non sono mancate, in dottrina, ricostruzioni indirizzate a riconoscere una rilevanza pubblica, sotto un profilo materiale, alle attività svolte nell'esercizio delle funzioni assegnate[360].

Tale rilevanza pubblica emerge con evidenza già solo allorché si prenda in considerazione la natura dell'organizzazione all'interno della quale il DPO svolge le proprie funzioni. Essa infatti può incidere anche significativamente sull'esercizio materiale dei compiti assegnati, in particolare nel rapporto con le relative finalità di rilievo giuspubblicistico[361].

Tuttavia, prima di approfondire una tale ricostruzione e passare in rassegna quelle funzioni che sembrerebbero determinare una caratterizzazione di tipo para-

---

[360] G. BELLOMO, *Contributo alla problematica della natura giuridica del "Data Protection Officer" (DPO)*, 26 marzo 2020, fruibile gratuitamente al *link* http://www.giurcost.org/LIBERAMICORUM/bellomo_scrittiCostanzo.pdf.

[361] ID., n. 38, p. 9: "*in tal senso va la stessa conformazione dell'organigramma del Garante che prevede Dipartimenti specifici e separati per le realtà economiche e produttive, per le realtà pubbliche, ma anche, tra gli altri, per sanità e ricerca. A riguardo si pensi, infatti: a quanto sia differente l'esercizio delle proprie funzioni per un DPO nel sorvegliare l'applicazione del Regolamento presso un soggetto privato che svolge attività d'impresa e presso un soggetto pubblico che persegue, invece, un fine di carattere pubblicistico; a come si possono modificare i livelli e le aree di rischiosità di disapplicazione del Regolamento, le dinamiche decisionali interne all'organizzazione e la tipologia e l'entità delle possibili conseguenze per gli interessati nelle due tipologie di organizzazione; ma anche alle profonde differenze esistenti nel trattamento dei dati anche tra organizzazioni pubbliche che possono essere profondamente diverse tra loro (si pensi ad esempio ad un ospedale, ad una università, ad un ministero o ad un comune)*".

pubblicistico di tale ruolo, si ritiene utile, al fine di offrire un'indagine quanto più esaustiva possibile, soffermarsi sulle affinità che, in virtù delle principali funzioni di carattere consultivo e di vigilanza, intercorrono tra il DPO e la figura dell'Organismo di Vigilanza ex D. Lgs. 231/2001.

2. Il *Data Protection Officer* e l'Organismo di Vigilanza: somiglianze e divergenze tra le due figure

Con il D. Lgs. 231/2001 è stata introdotta nel nostro ordinamento una nuova fattispecie di responsabilità amministrativa degli enti[362], dipendente da reati commessi «nell'interesse» o «a vantaggio» degli stessi, da parte di «soggetti in posizione apicale» ovvero di «soggetti sottoposti all'altrui direzione». Si tratta, com'è evidente, di una responsabilità distinta ed autonoma rispetto a quella delle persone fisiche appartenenti all'ente. Al fine di poter andare esente da responsabilità, infatti, l'ente dovrà dimostrare, ai sensi dell'art. 6 del citato decreto, di aver adottato un sistema organizzativo interno finalizzato garantire liceità e legittimità dell'attività d'impresa, attraverso la predisposizione ed attuazione di modelli di organizzazione, gestione e controllo (c.d. MOG) idonei a prevenire la commissione dei reati della specie di quello (eventualmente) verificatosi[363]. I modelli in questione, sostanzialmente, costituiscono una componente dei sistemi di controllo interno all'azienda[364], il cui fine è quello di

[362] La disciplina in questione trova applicazione non solo nei confronti degli enti forniti di personalità giuridica, ma anche delle società e associazioni prive di tale requisito. La giurisprudenza ha altresì esteso la responsabilità anche alle imprese individuali, nonché ai gruppi di società. Particolarmente significativo, al riguardo, appare il caso in cui la responsabilità venga fatta gravare sulla impresa controllante, allorquando il reato venga posto in essere da persone fisiche appartenenti all'organizzazione di quest'ultima, ma venga realizzato nell'interesse di una controllata. Cfr. Cass. Pen., sez. V, sent. 17/11/2010, n. 24583; Cass. Pen., sez. V, sent. 8/11/2012 n. 4324.

[363] I modelli in questione, che si ispirano ai *compliance programs* statunitensi, devono prevedere, in relazione alla natura ed all'estensione dei poteri delegati e al rischio di commissione dei reati:

a) l'individuazione delle attività nel cui ambito possono essere commessi reati;
b) specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
c) le modalità di individuazione e di gestione delle risorse finanziarie destinate all'attività nel cui ambito possono essere commessi reati;
d) obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
e) un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

[364] BASTIA*, I modelli organizzativi*, in AA. VV., *Reati e responsabilità degli enti*, Milano, 2005. La giurisprudenza ha già avuto modo di chiarire, in passato, che tali modelli devono prevedere, in relazione alla natura e alla dimensione dell'organizzazione, nonché al tipo di attività svolta, misure

prevenire eventuali situazioni di rischio. Già da questa considerazione può trarsi una prima affinità con la disciplina in materia di trattamento di dati personali, ove l'individuazione dei rischi cui il trattamento può incorrere, nonché l'adozione delle misure di sicurezza idonee ad eliminarli o prevenirli, non sono da soli elementi sufficienti a garantire una vera e propria *compliance* da parte del titolare del trattamento, e pertanto si è ritenuto necessario (almeno nelle realtà più complesse) fare in modo che l'attività del titolare fosse sottoposta a sorveglianza da parte di un soggetto terzo ed indipendente, appunto il DPO. In tema di responsabilità degli enti ex d.lgs. 231/2001, il legislatore ha ritenuto che l'adozione di un "modello" da parte dell'ente non costituisse da solo elemento sufficiente ad eliminare o arginare i rischi, dal momento che, per far sì che il modello venga concretamente ed efficacemente attuato[365], si stabilisce che ad un soggetto terzo, autonomo e indipendente, venga affidato il compito di vigilare sul

idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio. In quanto "*strumenti organizzativi della vita dell'ente*", i modelli, secondo la pronuncia in questione, "*devono qualificarsi per la loro concreta e specifica efficacia e per la loro dinamicità; essi devono scaturire da una visione realistica ed economica dei fenomeni aziendali e non esclusivamente giuridico-formale*". V. G.I.P. di Milano 20/09/2004 n. 30382-3, in Guida dir., n. 47/2004, p. 69 ss. Dall'analisi giurisprudenziale avente ad oggetto questioni interpretative legate all'adozione dei modelli, come già avuto modo di evidenziare Morezzi, "*in sintesi, la giurisprudenza richiede: un'analisi approfondita della realtà aziendale, delle caratteristiche del mercato di riferimento e delle possibili modalità attuative dei reati presupposto, la successiva parcellizzazione e procedimentalizzazione dei momenti della vita aziendali, la separazione dei compiti tra i soggetti coinvolti nelle fasi cruciali dei processi a rischio, la previsione di procedure di feed-back, la formazione specifica del personale esposto, un sistema disciplinare che sanzioni le manchevolezze degli addetti alle funzioni di controllo. In altre parole, di assetti organizzativi, amministrativi e tecnologici, adeguati alle esigenze di compliance espresse nel decreto. Il vaglio giudiziario sulla idoneità del modello è seguito da quello sulla effettiva attuazione dello stesso. Tutto ciò implica un'elevata formalizzazione del modello in fase di adozione ed attuazione, ma soprattutto che questo sia pienamente integrato nella operatività quotidiana dell'impresa. Solo a quest'ultima condizione è, infatti, possibile che gli obiettivi di compliance siano recepiti come componente costitutiva della cultura dell'impresa in cui si opera, le procedure non siano percepite come inutili fardelli burocratici, il modello di organizzazione non diventi un inutile e dannoso costo, si riesca effettivamente a prevenire la commissione di reati*". V. A. G. MOREZZI, *Modelli Organizzativi ex D. Lgs. n. 231/2001 e assetti adeguati ex art. 2381 c.c.: spunti di riflessione in tema di colpa di organizzazione*, in O. CAGNASSO – M. IRRERA, *Il Nuovo Diritto delle Società*, Numero 14/2008, p. 46.

[365] Per concreta attuazione del modello si deve intendere la necessità che lo stesso venga eventualmente modificato al ricorrere di particolari eventi. Scrive al riguardo Nisco "*il modello esige modifiche costanti, conseguenti ad eventi esterni e fisiologici, come l'ampliamento dell'organizzazione o la modifica delle attività, oppure "interni" e patologici, ossia le infrazioni ad esso riscontrate*". V. A. NISCO*, Responsabilità amministrativa degli enti: riflessioni sui criteri ascrittivi "soggettivi" e sul nuovo assetto delle posizioni di garanzia nelle società*, in *Riv. trim. dir. pen. econ.*, 2004, 293 ss.

funzionamento e sull'osservanza dello stesso, nonché quello di curarne l'aggiornamento.

Tale soggetto è, appunto, l'Organismo di Vigilanza (OdV)[366], il cui ruolo risulta rilevante ai fini della portata esimente del modello, tanto che il mancato o inefficiente adempimento dei compiti da parte dell'OdV (così come, a maggior ragione, la mancata nomina di un OdV a presidio del modello) renderebbe inefficace il modello medesimo, anche qualora quest'ultimo risultasse adeguato e completo sotto ogni altro punto di vista, e conseguentemente la responsabilità dell'ente non verrebbe meno. Ciò che deve essere evidenziato, in ogni caso, è che l'adozione del modello, e la correlata nomina dell'organismo, non costituiscono un obbligo per la società, ma un mero onere, che tuttavia risulta necessario e funzionale per poter essere la stessa esonerata dalla responsabilità amministrativa.

Con riferimento ai compiti assegnati all'OdV, occorre fare riferimento all'art. 6 del D. Lgs. 231/2001. Essi consistono nella vigilanza sull'osservanza del modello di prevenzione da parte di coloro che lavorano in ambito aziendale; nella verifica dell'efficacia di tale modello organizzativo, ossia la concreta idoneità dello stesso a prevenire il verificarsi dei reati enumerati nel decreto; nella cura dell'aggiornamento, qualora intervengano significative variazioni normative o modifiche del sistema organizzativo aziendale.

Emerge con evidenza, dunque, la scelta del legislatore di far dipendere la concreta efficacia del modello organizzativo dall'efficienza operativa della struttura di controllo, che dovrà svolgere sullo stesso una vigilanza di carattere continuativo.

Quanto ai requisiti propri di tale organismo, dall'enunciato dell'art. 6 è possibile ricavare che l'OdV debba essere dotato delle caratteristiche di indipendenza, autonomia e terzietà rispetto a coloro sui quali è chiamato a vigilare, e tali

---

[366] Sul tema, v., per tutti, FIORELLA, voce *Responsabilità da reato degli enti collettivi*, in Cassese (dir.), *Dizionario di diritto pubblico*, V, Milano, 2006, 5105; LA ROSA, *Teoria e prassi del controllo interno ed esterno sull'illecito dell'ente collettivo*, in *Riv. it. dir. proc. pen*., 2006, 1310 ss.; DE VERO, *La responsabilità penale delle persone giuridiche. Parte generale*, Milano,2008, 182 ss.; AA.VV., *Esperienze di avvio degli Organismi di Vigilanza* ex *d.lgs. 231/2001*, Quaderno n. 244, a cura del Centro Studi «Federico Stella» sulla Giustizia penale e la Politica criminale, 2008; MONTALENTI, *Organismo di Vigilanza e sistema dei controlli*, in *Giur. comm*., 2009, I, 643 ss.; PIERGALLINI, *I Modelli organizzativi*, in LATTANZI (a cura di), *Reati e responsabilità degli enti*, 2a ed., Milano, 2010, 173 ss.; MUCCIARELLI, *Funzioni e responsabilità dell'organismo di vigilanza*, in A.M. STILE, V. MONGILLO, G. STILE (a cura di), *La responsabilità da reato degli enti collettivi: a dieci anni dal d.lgs. 231/2001. Problemi applicativi e prospettive di riforma*, Napoli, 2013, 197 ss.

requisiti debbano sussistere sia nel caso in cui a comporre l'organismo siano soggetti interni alla società (nella quale si trova poi ad operare), sia nel caso in cui si tratti di soggetti esterni.

Nonostante gli elementi citati, e sebbene il compito di vigilanza risulti affidato dalla legge, occorre tuttavia rilevare come a quest'onere di controllo non si accompagni altresì la previsione di poteri di carattere impeditivo, disciplinare o sanzionatorio nei confronti di comportamenti illeciti posti in essere dagli organi apicali o dai dipendenti; ed emerge su questo profilo un secondo punto di affinità con la figura del DPO, al quale la legge, pur indicando alcuni requisiti e compiti caratterizzanti, non riconosce poteri di intervento volti, rispettivamente, ad obbligare il titolare del trattamento a conformarsi a quanto suggerito dallo stesso DPO nell'espletamento del proprio mandato ovvero a impedirgli di porre in essere azioni ritenute illecite o perseguire nelle lacune e/o violazioni eventualmente riscontrate.

Né viene previsto, in capo all'OdV, un obbligo di comunicazione alle Autorità pubbliche in merito ad eventuali illeciti riscontrati nel corso dell'attività ispettiva, salvo alcune eccezioni: ci si riferisce alla disciplina in materia di antiriciclaggio, delineata nel D. Lgs.21 novembre 2007, n. 231. L'art. 52 del menzionato decreto, infatti, determina una sorta di trasfigurazione dell'ordinaria fisionomia dell'OdV, il quale non assume più il ruolo di mero assegnatario di doveri di vigilanza a rilevanza puramente interna, ma si rivolge anche all'esterno, data la previsione dell'obbligo di comunicare alle Autorità pubbliche preposte alla sorveglianza ed al contrasto delle attività illecite di riciclaggio, come specificate nella norma, tutti gli atti o i fatti di cui sia venuto a conoscenza nell'esercizio dei propri compiti e che possono costituire, appunto, una violazione delle disposizioni emanate dal decreto antiriciclaggio[367].

La dottrina si è interrogata molto su tale disposizione, chiedendosi se dalla stessa debba farsi discendere una posizione di garanzia rilevante ai sensi dell'art. 40 c.p. o se, piuttosto, la norma debba essere letta nel senso che sull'OdV graverebbe un

[367] Le autorità cui fa riferimento la norma sono le autorità di vigilanza di settore, nonché il Ministero dell'economia e delle finanze e l'UIF (Unità di Informazione Finanziaria presso la Banca d'Italia). La norma stabilisce ulteriormente che l'OdV sarà tenuto a comunicare, senza ritardo, anche al titolare dell'attività o al legale rappresentante o a un suo delegato, le infrazioni alle disposizioni concernenti la segnalazione di operazioni sospette di cui ha notizia.

mero onere di segnalazione/avviso ad altri soggetti, unici deputati ad intervenire per accertare e sanzionare l'illecito[368]. Tralasciando il dibattito dottrinale in merito alla sussistenza o meno di una posizione di garanzia in capo all'organismo, che comunque viene esclusa dai più[369], ciò che rileva ai fini della presente indagine è l'introduzione della possibilità data all'OdV di comunicare direttamente con le pubbliche autorità competenti, le quali potranno utilizzare le relative comunicazioni come elementi d'indagine (mentre, nella disciplina "ordinaria", i risultati dei controlli restavano all'interno dell'organizzazione); non sfugge, tuttavia, come una tale considerazione possa modificare (addirittura "snaturare") almeno in parte la natura dell'OdV, conferendogli, come già evidenziato, una rilevanza non meramente interna, ma anche esterna.

Da quanto sin qui esposto, è evidente come l'OdV, nel sistema del D. Lgs. 231/2001, ed il DPO, nelle logiche del GDPR, rappresentino organi con funzioni di chiusura dei rispettivi sistemi. Questi condividono, come anticipato, i medesimi paradigmi strutturali, tanto che possono essere riferite anche al DPO le riflessioni che la dottrina ha già svolto in relazione all'OdV, allorquando ha sostenuto che «la «fisionomia identitaria» dell'OdV risulta sospesa tra due diversi paradigmi strutturali di controllo: quello del compliance officer, che per semplicità potremmo chiamare il «paradigma funzionale», e quello dell'organo di controllo societario, «paradigma istituzionale-societario». Questa enigmaticità, a ben vedere, era ab origine insita nella «duplice anima» dell'OdV ex d.lgs. 231/2001, le cui competenze ibridano funzioni di vigilanza ispettiva, tipiche di un soggetto terzo e indipendente, e funzioni consulenziali e informative, tipiche di un ufficio di supporto»[370].

Entrambi gli uffici sono caratterizzati dai requisiti dell'autonomia e dell'indipendenza, sia con riferimento alla loro collocazione nell'organigramma

---

[368] Cfr. A. BAUDINO – C. SANTORIELLO, *La responsabilità dei componenti dell'Organismo di Vigilanza*, in *Resp. Amm. Enti*, 2009, II, 66; F. D'ARCANGELO*, Il ruolo e la responsabilità dell'Organismo di Vigilanza nella disciplina antiriciclaggio*, in *Resp. Amm. Enti*, 2009, I, 68 ss.

[369] Secondo l'indirizzo dottrinario dominante, quella dell'OdV non si ritiene essere una posizione integrante gli estremi dell'obbligo di protezione, bensì dell'obbligo di controllo tipico dell'organismo, preordinato all'impedimento dell'attività criminosa altrui. I poteri di impedimento del fatto continueranno infatti a gravare sui titolari della gestione della società, in cui l'OdV non può ingerirsi.

[370] V. V. MONGILLO, *L'organismo di Vigilanza nel sistema della responsabilità da reato dell'ente: paradigmi di controllo, tendenze evolutive e implicazioni penalistiche*, in *Responsabilità amministrativa delle società e degli enti (La)*, 2015, *n.* 4.

della società o ente, sia con riferimento allo svolgimento dei compiti che sono loro demandati, il principale dei quali risulta essere quello di controllo, che viene svolto secondo il medesimo approccio funzionale, focalizzato sulla prevenzione del rischio (*risk based approach*) e finalizzato, da un lato, ad evitare il compimento di reati, e dall'altro a garantire un corretto trattamento dei dati raccolti da un'azienda.

A ragione del diverso ambito operativo, i due organismi, inoltre, sono spesso chiamati a collaborare tra loro nelle realtà aziendali: il DPO, infatti, incontra periodicamente l'OdV per riferire sullo stato di attuazione del sistema di protezione dei dati personali, nonché per segnalare eventuali criticità emerse e violazioni oggetto di fattispecie prevista dal D. Lgs. 231/2001, oppure ancora per l'aggiornamento del MOG e per garantire la riservatezza delle segnalazioni destinate all'OdV.

Tuttavia, come già si è rivelato, contrariamente a quanto avviene per il DPO, la nomina dell'OdV non è prevista dalla legge come obbligatoria: la stessa, piuttosto, costituisce un onere che, se assolto, determina la possibilità per l'ente di non andare incontro a responsabilità amministrativa, nel caso in cui i soggetti alle proprie dipendenze pongano in essere un reato a vantaggio di quest'ultimo. L'OdV, dunque, è una figura istituita principalmente a tutela di un interesse prettamente interno, che è quello dell'ente in cui opera: la sua presenza, infatti, mira a garantire che il sistema interno di prevenzione dei reati sia un sistema effettivamente valido a prevenire il compimento dei fatti illeciti indicati nel decreto.

Il DPO, al contrario dell'OdV, è una figura da nominare obbligatoriamente in ogni entità pubblica ed in quelle private che effettuino trattamenti di dati personali particolarmente rischiosi, ciò in quanto si ritiene che, in tali realtà, l'interesse dei soggetti cui i dati personali vengono trattati possa essere meglio tutelato non solo attraverso gli accorgimenti e gli obblighi imposti dalla legge al titolare, ma altresì in ragione della presenza di un soggetto dotato delle competenze professionali idonee a coadiuvare nel migliore dei modi il titolare del trattamento, e a vigilare sull'operato dello stesso.

Il diritto alla protezione dei dati personali, infatti, viene garantito dal fatto che il DPO, con la sua presenza ed il suo operare nell'ente, assicura la *compliance* del titolare rispetto alla legge: attraverso il perseguimento dell'interesse privato del titolare si giunge così a tutelare il differente interesse pubblico alla protezione dei dati personali, appartenente a tutti gli interessati e, più in generale, a tutti coloro i quali possano riferirsi situazioni giuridiche rilevanti connesse con le attività di trattamento.

La mera presenza del DPO, espressione dell'assolvimento dell'obbligo gravante *ex lege* sul titolare, non garantirà la possibilità per quest'ultimo di andare, in ogni caso e con certezza, esente da qualsiasi responsabilità, nel caso di situazioni di *data breach* o di altri illeciti che possano determinare danni agli interessati od a soggetti terzi, specie in tutti quei casi in cui egli non si sia attenuto alle indicazioni offerte dal DPO, dovendo in tal caso addurre le motivazioni che lo hanno indotto a non conformarvisi.

Ancora, ciò che sembra ulteriormente distinguere le due figure dell'OdV e del DPO, è la segnalata funzione di cooperazione con l'Autorità Garante (art. 39, lett. d). Si è già rilevato come, solo con riferimento alla disciplina antiriciclaggio, venga in rilievo un obbligo di cooperazione dell'OdV con le Autorità pubbliche di vigilanza, in virtù del quale il primo è tenuto a segnalare alle seconde le condotte illecite di cui sia venuto a conoscenza. Con riferimento al DPO, l'obbligo di cooperazione non si sostanzia in un obbligo di segnalazione di eventuali comportamenti illeciti riscontrati nel corso della vigilanza, atteggiandosi piuttosto come attività di supporto all'Autorità nel momento in cui la stessa proceda a dei controlli, ovvero nell'avanzamento di richieste di natura consulenziale a quest'ultima al fine di meglio coadiuvare il titolare.

In argomento, tuttavia, ci si chiede se non possa ritenersi migliorativo della disciplina normativa di riferimento un intervento teso ad introdurre, anche in riferimento alle attività di controllo e vigilanza del DPO, un simile ed eventuale obbligo di segnalazione. Con la doverosa premessa che una tale previsione dovrebbe poi definire compiutamente le ipotesi (o almeno le macro-aree) di intervento e segnalazione, una tale innovazione potrebbe apparire utile, specie in considerazione delle realtà pubbliche in cui il DPO viene ad operare, e ancor di

più, nei casi in cui si tratti di un DPO interno, cioè dipendente del suddetto ente, anche in considerazione di una possibile rilettura dell'obbligo di cooperazione, che si tenterà di offrire nei prossimi paragrafi.

3. La funzione di cooperazione con l'Autorità di controllo: il *Data Protection Officer* come *longa manus* del Garante?

L'obbligo di cooperazione con il Garante, sancito dall'art. 39 c.1, lett. d), è uno dei profili che caratterizza maggiormente la figura del DPO, differenziandola dalle altre figure incaricate a vario titolo di assicurare la *compliance* del datore di lavoro (o titolare del trattamento, allorché si discuta di protezione dei dati personali).

Da tale circostanza deriva la necessità di concentrare maggiormente l'attenzione sul modo in cui si esplica tale funzione di cooperazione, poiché la stessa sembra avere delle importanti ricadute in punto di qualificazione giuridica del ruolo in esame. L'analisi che si intende svolgere mira ad offrire degli spunti per un tentativo di definizione della posizione del DPO rispetto sia al tema dell'interesse da questi protetto, sia a quello inerente il ruolo che questi viene ad assumere nell'ambito dell'organigramma dell'ente in cui è chiamato ad operare.

Sorge spontaneo, infatti, domandarsi se, in virtù di tale obbligo, nonché in considerazione dell'intreccio tra questo e gli ulteriori adempimenti cui il DPO è tenuto, egli vada considerato alla stregua di un professionista, dotato di competenze specialistiche, che una volta nominato dal titolare assuma le vesti di consulente di quest'ultimo con rilevanza solo interna, e dunque caratterizzandosi come organismo di tipo privatistico, o se, piuttosto, ci si possa spingere sino al punto di considerarlo una sorta di "autorità interna" nell'ambito dell'azienda o dell'ente pubblico, che potrebbe agire in qualità di *longa manus* dell'Autorità Garante.

Nel caso in cui si aderisse a tale ultima lettura interpretativa, occorrerebbe altresì valutare se e come tale configurazione del DPO quale "estensione" dell'Autorità, possa andare ad incidere su eventuali profili di diligenza e responsabilità inerenti lo stesso, sia, ulteriormente ed in via eventuale, su eventuali profili di responsabilità del titolare.

In merito a tale interpretazione, inoltre, si vuole evidenziare come, sebbene la stessa possa essere ritenuta, per certi versi, "audace", anche alla luce delle previsioni normative dettate in materia, tuttavia non sono mancate voci della dottrina che abbiano sostenuto come la professione in esame non possa essere considerata solo un'attività lavorativa, ma piuttosto vada interpretata come una vera e propria "funzione"[371], volendo con ciò intendere che tale ruolo assume, inevitabilmente, un rilievo di carattere "pubblicistico", poiché esso opera non solo nell'interesse del titolare, ma, anzi, e principalmente, nell'interesse di coloro ai quali i dati personali appartengono e, più in generale (per i profili messi in rilievo nel secondo capitolo), dell'intera comunità [372].

Certo è che, anche allorquando non si volesse far discendere dalla funzione di cooperazione la natura pubblicistica del ruolo del DPO, tuttavia, il contenuto della stessa merita di essere comunque approfondito, anche al fine di suggerire eventuali apporti migliorativi della disciplina.

Ci si potrebbe chiedere, infatti, se, in relazione al mancato o inesatto adempimento dei compiti che si ritiene presentino un nesso, anche solo indiretto, con tale funzione di cooperazione, possa essere ipotizzata la possibilità di configurare eventuali profili di responsabilità esclusiva in capo al DPO nei confronti dei soggetti interessati o nei confronti della stessa Autorità, oppure ancora quella di tenere indenne il titolare del trattamento dalla responsabilità che verrebbe a gravare in capo a questi per violazione delle norme di legge, o, quanto meno, al fine di evitare che a questi vengano comminate le sanzioni amministrative di cui all'art. 83 GDPR[373].

---

[371] V. F. PIZZETTI, *Gdpr, ecco le vere funzioni del DPO: "attenti, non è un mestiere"*, rinvenibile al link *https://www.agendadigitale.eu/sicurezza/gdpr-attenti-fare-il-dpo-non-e-un-mestiere-ecco-le-sue-vere-funzioni/*.

[372] *Ibidem*.

[373] L'art. 83 GDPR, rubricato "*Condizioni generali per infliggere sanzioni amministrative pecuniarie*", disciplina le modalità di applicazione delle sanzioni amministrative che devono essere inflitte in occasione di ogni violazione del Regolamento. Non vengono stabilite fattispecie tipiche, ma vi è un'indicazione generica e omnicomprensiva che abbraccia ogni ipotesi di violazione. Nei casi in cui l'Autorità di controllo, a seguito di reclamo ai sensi dell'art. 77 del Regolamento o di attività istruttoria di sua iniziativa (nell'ambito dei poteri di indagine di cui all'art. 58, par. 1, del Regolamento), nonché in occasione di accessi, ispezioni e verifiche svolte in base a poteri di accertamento autonomi, dovesse riscontrare la violazione, provvederà all'inflizione della relativa sanzione, nel rispetto dei princìpi dettati dal summenzionato art. 83. Cfr. G. M. RICCIO – G. SCORZA – E. BELISARIO, *GDPR e normativa privacy, Commentario*, Wolters Kluwer, 2018, pp. 604-613.

È chiaro, tuttavia, con riferimento alle ipotesi in cui dalla violazione dovesse derivare un danno agli interessati, che la paventata possibilità di una responsabilità del DPO nei loro confronti, che potrebbe configurarsi difficilmente come esclusiva, e più agevolmente come concorrente con quella del titolare, appare ben ardua da concretizzare, stante le maglie alquanto restrittive del Regolamento, sebbene non per questo assolutamente impossibile.

3.1 Il contenuto dell'obbligo di cooperazione del DPO nei confronti del Garante

Al fine di comprendere l'incidenza dell'obbligo di cooperazione di cui all'art. 39 GDPR sulla natura dell'incarico di DPO, è bene passare in rassegna le norme del GDPR che prevedono e disciplinano espressamente i casi in cui questi è tenuto ad interagire e/o collaborare con il Garante. Il GDPR, infatti, nel sancire tale obbligo, non ne specifica con precisione il contenuto, né opera un rinvio esplicito alle norme che verranno analizzate nel prosieguo. L'art. 39, infatti, opera secondo il modello della c.d. "norma in bianco": in virtù di questa previsione, il DPO, a sua discrezione, potrà consultare gli uffici del Garante in merito a qualsiasi questione, ove lo ritenga opportuno.

Nonostante l'astrattezza della norma richiamata, si può comunque fare riferimento a due casi specifici in cui il GDPR prevede la cooperazione tra DPO e Autorità, che riconducono a due momenti diversi del trattamento, uno fisiologico ed uno patologico, uno preventivo e l'altro successivo. Il primo viene in riferimento nell'ambito del D.P.I.A. (*Data Protection Impact Assessment*); il secondo, invece, nel caso in cui il titolare del trattamento subisca un *data breach*.

In entrambi i casi, al ricorrere di determinate circostanze, il titolare del trattamento sarà tenuto a comunicare al Garante i dati di contatto del DPO, affinché l'Autorità possa interloquire con un soggetto che, essendo dotato di competenze specialistiche, è l'unico realmente in grado di fornire all'Autorità ogni chiarimento reso necessario dalle particolari situazioni cui si fa riferimento.

3.1.1 L'obbligo di cooperazione nel D.P.I.A.

Con riferimento al D.P.I.A., si è già avuto modo di specificare che il *Data Protection Impact Assestment* consiste in una valutazione dei rischi condotta dal titolare in relazione a tutti quei trattamenti a maggior rischio di impatto sulle libertà e i diritti fondamentali degli interessati, rispetto ai quali lo stesso titolare è obbligato ad individuare le misure di sicurezza utili ad abbattere o mitigare tale rischio, prima di dar luogo al trattamento in questione[374]. Nello svolgimento del D.P.I.A., il titolare viene coadiuvato dal DPO, al quale può chiedere in qualsiasi momento il rilascio di un parere, che questi è obbligato a fornire ai sensi dell'art. 39 lett. c). Tale parere potrebbe avere ad oggetto, a titolo esemplificativo, o la valutazione circa la conformità di un determinato trattamento ai requisiti previsti *ex lege*, oppure l'idoneità o meno delle misure di sicurezza individuate dal titolare per evitare o arginare i rischi preventivati. In questa fase, dunque, il ruolo del DPO viene in rilievo principalmente in considerazione della sua funzione consulenziale (art. 39, lett. a).

L'attività di collaborazione con il Garante, infatti, avrà luogo soltanto in un eventuale momento successivo, allorquando, cioè, il titolare ritenga che, nonostante le misure di sicurezza individuate per mitigare il rischio, lo stesso continui a restare "elevato", mettendo così a repentaglio la possibilità di dar luogo al trattamento oggetto di valutazione. In tal caso, il titolare è tenuto a richiedere una consultazione preventiva all'Autorità ai sensi dell'art. 36 GDPR, indicando a questa il contatto del DPO, che sarà il soggetto incaricato a rappresentare eventuali scelte organizzative e/o tecniche attuate dal Titolare.

Pertanto, nell'ambito del D.P.I.A., la funzione di cooperazione tra DPO e Autorità sembra venire in rilievo solo una volta che il titolare si sia attivato nel chiedere un consulto a quest'ultima.

Tuttavia, è necessario porre particolare attenzione alla fase temporale che si colloca tra la fine della valutazione di impatto e quella dell'eventuale consultazione, poiché è proprio questa la fase in cui, generalmente, il titolare

[374] Si rinvia al Cap. II, par. 5.3.

richiede al DPO il rilascio di un parere circa la necessità o meno di detta consultazione[375].

Inoltre, anche nel caso in cui il parere non venga esplicitamente richiesto dal titolare, il DPO, in virtù dell'onere di sorveglianza, che rientra fra i suoi compiti (e che, come si è rilevato, incide su ogni operazione inerente il trattamento posta in essere dal titolare e dunque, a maggior ragione, sulla fase della valutazione d'impatto), sarebbe comunque tenuto ad attivarsi, esprimendosi in merito alla necessità o meno di procedere a detta consultazione. Ed è proprio nel rilascio del parere in questione, stante tutte le implicazioni che ne derivano, che può essere rintracciato, a parere di chi scrive, l'ulteriore significato da attribuire all'obbligo di cooperazione oggetto di indagine, svincolando così tale obbligo dalla mera attività collaborativa che si origina soltanto a seguito dell'avvio della consultazione da parte del titolare.

Nel momento in cui il titolare decida di coinvolgere il DPO chiedendo il parere in merito alla necessità di procedere alla consultazione ex art. 36 GDPR quest'ultimo potrà suggerire di procedervi o di non procedervi ed il titolare, a sua volta, potrà decidere di conformarsi o meno al parere dato. Generalmente, tenderà a conformarsi ad esso, anche perché, qualora non dovesse farlo, dovrà rispondere delle proprie scelte dinanzi all'Autorità, in un eventuale momento successivo[376].

---

[375] Come già evidenziato, il legislatore prevede che, durante lo svolgimento della valutazione d'impatto, ovvero al suo termine, il Titolare possa richiedere al DPO il rilascio di pareri, che questi fornisce, sostanzialmente, in qualità di consulente. In particolare, il parere potrebbe avere ad oggetto la necessità o meno, secondo il DPO, di procedere alla consultazione preventiva del Garante ai sensi dell'art. 36 GDPR. È bene però sottolineare che non sempre il Titolare può ritenere di dover richiedere tale parere: tale decisione, al pari di varie altre che vengono in rilievo nell'ambito della gestione del trattamento dei dati, deve essere conformata al principio di *accountability* che ispira l'intera normativa. Nel caso in cui il Titolare decida di non richiedere il parere del DPO, e magari non procedere alla consultazione preventiva dell'Autorità, oppure di richiederlo e non attenersi alle sue indicazioni circa la necessità di procedere a consultazione preventiva, dando comunque avvio al trattamento, potrà eventualmente rispondere del suo operato, se in un momento successivo l'Autorità dovesse ritenere che le circostanze avrebbero reso necessario il suo intervento (si pensi al caso in cui il Titolare, operando una valutazione costi-benefici, ritenga, al termine della valutazione d'impatto, che, sebbene il trattamento si presenti come altamente rischioso, alla luce del profitto che potrebbe derivargliene decida di attuarlo comunque, omettendo la consultazione preventiva per non correre il rischio di vedersi negata l'autorizzazione).

[376] Si pensi, in particolare, al caso in cui il DPO ritenga necessaria la consultazione preventiva dell'Autorità, ma il Titolare decida di non attenersi al parere e di non procedere a consultazione, dando comunque avvio al trattamento. È chiaro che, in tal caso, il Titolare accetta la possibilità che si verifichi un danno ai diritti dei soggetti interessati, da ciò derivando anche una responsabilità di questi in sede civile o penale. La peculiarità di tale circostanza sarà oggetto di indagine nel prossimo paragrafo.

A tal riguardo, ci si chiede quale possa essere la conseguenza nell'ipotesi in cui il DPO dovesse ritenere superfluo procedere alla consultazione preventiva e, a seguito di un accertamento ispettivo da parte dell'Autorità (ad esempio a causa del verificarsi di un *data breach*, cioè di una violazione), la stessa dovesse ritenere che la consultazione preventiva fosse da considerarsi un passaggio obbligato, e che il parere del DPO sia stato dunque reso in maniera negligente, imprudente o imperita, determinando così il titolare a dar luogo al trattamento senza coinvolgere preventivamente l'Autorità.

Ai sensi della disciplina dettata dal GDPR, il titolare, che si è affidato alla consulenza del DPO, verrà ritenuto responsabile nei confronti degli interessati che dovessero subire un danno in virtù del trattamento non preventivamente autorizzato, e che magari l'Autorità non avrebbe autorizzato affatto.

Inoltre, sorge il dubbio sulla possibilità che, anche a prescindere da eventuali danni ai soggetti interessati, il titolare possa comunque andare incontro ad una sanzione amministrativa a seguito dell'accertamento ispettivo, per aver posto in essere il trattamento che andava segnalato.

Ci si chiede se, nelle ipotesi delineate, il titolare potrà ritenersi esonerato, dimostrando che l'evento dannoso non gli è in alcun modo imputabile, stante la circostanza per cui, qualora il DPO avesse agito con diligenza nel rilascio del parere in esame, evidenziando la necessità di una consultazione preventiva dell'Autorità, egli vi avrebbe certamente provveduto.

Questa riflessione potrebbe essere soggetta a critiche dal momento che, così argomentando, il titolare potrebbe sempre essere tenuto indenne da qualsiasi responsabilità, o per lo meno da qualsiasi sanzione di carattere amministrativo, nel caso in cui il DPO non adempisse diligentemente ai propri doveri. Tuttavia, per ribattere a tale considerazione, si potrebbe ipotizzare il verificarsi della seguente fattispecie: si pensi al caso in cui il DPO venga incaricato dal titolare della gestione del registro dei trattamenti, di cui all'art. 30 GDPR (compito che la legge fa gravare sul titolare ma che, nella prassi, viene spesso affidato al DPO). Qualora il DPO dovesse non adempiere con diligenza all'aggiornamento e alla cura del registro in questione, il titolare, eventualmente sanzionato ai sensi dell'art. 83 GDPR, non potrà andare esente da responsabilità, stante l'obbligo, su sé gravante,

di mantenere un controllo sul puntuale adempimento dei compiti da parte del DPO, specie in ipotesi di compiti di carattere operativo, e a maggior ragione se la legge individua, proprio nel titolare, il principale obbligato. Di certo, una volta sanzionato, egli potrà comunque rivalersi sul DPO.

Diverso è il caso in cui, invece, il DPO non adempia diligentemente alla funzione consultiva e, nello specifico, a quella presa in considerazione nell'esempio di cui sopra, nell'ambito del D.P.I.A.

In tal caso, infatti, il DPO non agisce come incaricato di un compito di carattere meramente operativo, né come "semplice" consulente qualificato del titolare, ma, ed è questa la teoria che si vuole sostenere circa l'interpretazione da dare all'obbligo di cooperazione, sostanzialmente come referente dell'Autorità di controllo, allorché tale obbligo di cooperazione sia oggetto di un'interpretazione più ampia.

Il parere del DPO, infatti, sarà determinante con riferimento alla possibilità per l'Autorità di intervenire a monte del trattamento, ai fini di una idonea salvaguardia dell'interesse pubblico alla protezione dei dati personali. Se il DPO, negligentemente, dovesse ritenere tale intervento superfluo, e il titolare (che riponga la propria fiducia nelle sue competenze) decidesse di adeguarsi a tale parere, verrebbe ad aumentare l'indice di rischio al quale risulterebbero esposti i dati degli interessati. La presenza del DPO nelle realtà aziendali e negli enti pubblici , soprattutto con riguardo a quelle realtà che pongono in essere trattamenti particolarmente rischiosi, da circostanza idonea a fungere da garanzia circa l'attuazione della migliore tutela possibile dell'interesse pubblico, diverrebbe così elemento ostativo ad ottenere la tutela di stampo pubblicistico, stante la possibilità di influenzare, impedendolo, l'intervento dell'Autorità di controllo che, nei casi in esame, dovrebbe vigilare a monte, e non soltanto *ex post*, sull'operato del titolare.

Ciò che si vuole sostenere è che il DPO, nell'ipotesi appena passata in rassegna, dovrebbe ritenersi obbligato ad adempiere il proprio incarico in maniera diligente non soltanto in virtù del contratto intercorrente con il titolare e per le eventuali conseguenze da inadempimento che potrebbero derivarne, ma anche e soprattutto in considerazione del fatto che, nei casi come quello attenzionato, egli

sembrerebbe rivestire prevalentemente la funzione di referente del Garante, il cui potere di intervento, nei casi in questione, è condizionato proprio dal parere rilasciato dal DPO, poiché è ragionevole immaginare che il titolare, affidandosi a questi, potrebbe non procedere alla consultazione.

3.1.2 L'obbligo di cooperazione nel *data breach*

Così analizzato il primo caso di attività di collaborazione sancito *ex lege*, occorre ora passare in rassegna il secondo, vale a dire l'ipotesi in cui il titolare subisca un *data breach*: una violazione della sicurezza, accidentale o illecita, che determina la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Nel momento in cui il titolare viene a conoscenza della violazione, ai sensi dell'art. 33 GDPR, dovrà provvedere a notificare detta violazione all'Autorità di controllo, senza ingiustificato ritardo e, ove possibile, entro 72 ore, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Nell'atto di notificazione, il titolare è tenuto ad indicare i dati di contatto del DPO, affinché questi collabori con l'Autorità. Anche in questo caso viene in rilievo quanto già evidenziato con riferimento al parere rilasciato dal DPO al termine del DPIA.

Ai sensi dell'art. 33, infatti, il titolare non è tenuto alla notifica della violazione, allorquando sia improbabile che la stessa determini un rischio per i diritti e le libertà delle persone fisiche. In tal caso, il titolare potrà decidere direttamente di notificare, senza richiedere un previo parere al DPO al riguardo, ovvero (e, nella prassi, è naturale attendersi che sia questa l'opzione più frequente) chiedere allo stesso un preventivo parere circa l'obbligo di provvedere o meno alla notifica. Emerge tuttavia un profilo di dubbio, in relazione all'ipotesi in cui il DPO dovesse ritenere non necessaria la notifica, e dunque il titolare, attenendosi a tale parere, non vi provveda, e l'Autorità, invece, dovesse decidere di intervenire, in un momento successivo, valutando la mancata notifica in termini di violazione dell'obbligo e quindi operando una valutazione discorde da quella fatta dal DPO. In una tale ipotesi, viene da chiedersi se il titolare dovrebbe essere sanzionato ai sensi dell'art. 83 GDPR, o potrebbe, invece, andare esente da responsabilità,

proprio in virtù dell'affidamento nei confronti della valutazione del DPO. In relazione a quest'ultimo, ancora, resta da chiedersi se dovrà rispondere dell'operato, che ha esposto alle sanzioni, il titolare, e se tale responsabilità potrà configurarsi come mancato o inesatto adempimento.

Peraltro, nel caso di *data breach*, potrebbe venire in rilievo un'ulteriore evenienza, sicuramente più inerente l'obbligo di cooperazione inteso *strictu sensu*. Nell'espletamento dell'attività collaborativa, e nello specifico, nell'obbligo di rendere all'Autorità eventuali chiarimenti di cui la stessa dovesse aver bisogno, il DPO dovrà comportarsi secondo un canone di diligenza professionale, ma viene da chiedersi cosa potrebbe accadere in caso di mancata attivazione o di adempimento in maniera inesatta. Se è pur vero che l'Autorità potrà rivolgersi al titolare, ed è altresì vero anche che questi potrà eventualmente agire contro il DPO, il dubbio che si pone risiede sulla possibilità che sia comunque il titolare ad andare incontro ad eventuale sanzione per il mancato rispetto delle norme di legge, essendo così chiamato a rispondere per l'inadempimento del DPO[377].

Stesso interrogativo potrebbe poi sorgere con riferimento all'atto di notifica all'Autorità dell'avvenuto *data breach,* dal momento che il contenuto della notifica, infatti, viene redatto dal titolare con la collaborazione del DPO, se non, presumibilmente (in qualsiasi tipo di realtà presa in considerazione, sia essa pubblica o privata), in via esclusiva da quest'ultimo[378]. Del resto, è difficile credere che il titolare abbia le competenze idonee a soddisfare l'obbligo, sancito dallo stesso art. 33, di "descrivere la natura della violazione dei dati personali

[377] Si rende necessario proporre un esempio: si pensi ad uno studio medico, in cui viene nominato un consulente *privacy* che, in sostanza, si ritrovi a svolgere le concorrenti funzioni di DPO, in ragione della necessità di un mantenimento dei costi aziendali tale per cui non è possibile nominare più soggetti. Qualora lo studio in questione dovesse subire un *data breach*, e abbia dato notizia dello stesso all'Autorità, nel caso in cui questa abbia la necessità di ottenere determinate informazioni inerenti la violazione, solo il DPO si troverà nelle condizioni di poter rispondere compiutamente alle richieste dell'Autorità, non essendovi altri soggetti deputati a farlo.

[378] L'art. 33 stabilisce che la notifica deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze delle violazioni dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, per attenuarne i possibili effetti negativi.

compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione". Generalmente, il titolare potrà fare riferimento agli addetti alla gestione tecnica dei sistemi di sicurezza, confrontandosi direttamente con loro, ma è evidente, oltre che più probabile, che sia il DPO a fungere da punto di contatto per gli stessi incaricati, rientrando anche tale funzione tra i suoi compiti. Pertanto, quasi sicuramente, sarà il DPO a dover provvedere all'onere di redigere il contenuto della notifica in questione. In tal caso, è naturale domandarsi cosa potrebbe avvenire nell'ipotesi in cui la notifica sia carente di un contenuto prescritto *ex lege*, che, nonostante le sollecitazioni dell'Autorità, il DPO non provveda ad aggiornare, ed in particolare è da chiedersi se sarà, ancora una volta, il titolare ad essere sanzionato per l'eventuale inadempimento del DPO.

Ancora, l'art. 33, al par. 5, prevede che il titolare del trattamento documenti qualsiasi violazione di dati personali, compresi le circostanze a essa relative, le conseguenze e i provvedimenti adottati per porvi rimedio. Anche in tal caso, è altamente probabile che, nelle realtà prese in considerazione, il compito di redigere tale registro possa esser fatto gravare sul DPO, conformemente a quanto accade con riferimento al registro di cui all'art. 30 GDPR.

Certo è che, nelle ultime due ipotesi attenzionate, si è dinanzi a compiti di carattere operativo che, ai sensi di legge, sarebbero posti in via esclusiva in capo al titolare, sebbene questi, in totale autonomia, possa decidere di delegarli al DPO. Pertanto, al ricorrere di queste ultime circostanze, è legittimo ipotizzare che il DPO sarà sicuramente tenuto a rispondere per inadempimento contrattuale nei confronti del titolare e che, tuttavia, quest'ultimo potrebbe legittimamente essere sanzionato dall'Autorità (sebbene a causa dell'inadempimento o l'inesatto adempimento del primo).

3.1.3 L'obbligo di cooperazione nei casi di condotta colpevole del *Data Protection Officer*

Alla luce dell'interpretazione offerta in merito all'obbligo di cooperazione, appare lecito domandarsi se lo stesso, nel significato che si è inteso attribuire, eserciti un'influenza particolare sulla natura giuridica del ruolo del DPO ed

eventualmente anche sui profili di responsabilità ad esso correlati. Del resto, tale obbligo, come si è visto, viene sancito dall'art. 39 lett. d), ma la norma, come già evidenziato, non ne specifica né il contenuto, né opera, a tal fine, un richiamo diretto e univoco ad altre specifiche norme del GDPR. Di certo, le norme attenzionate nei paragrafi precedenti (artt. 33 e 36 GDPR), prevedono una necessaria attività collaborativa tra DPO e Autorità, che prenderebbe avvio nel momento in cui il titolare comunica a quest'ultima i dati di contatto del DPO. Se l'obbligo di cooperazione si limitasse a tale attività collaborativa, è evidente come non potrebbe sorgere alcun dubbio circa la configurazione del DPO quale ufficio avente rilevanza meramente interna all'ente in cui viene ad operare e che si limita a facilitare le comunicazioni tra Autorità ed organizzazione.

Tuttavia, come si è avuto modo di sottolineare, non sembra che l'interpretazione dello stesso possa esaurirsi in una collaborazione, di carattere principalmente tecnico, successiva alla notifica, ritenendo piuttosto che il vero portato andrebbe rintracciato nel momento antecedente, vale a dire quello del rilascio del parere al titolare. Questo è il momento in cui il DPO è chiamato a garantire i diritti degli interessati, attraverso una valutazione circa la necessità o meno di far intervenire l'Autorità pubblica. Se, con il suo operato negligente, egli dovesse ritenere la consultazione preventiva non necessaria, precludendo così l'intervento pubblico, e dunque anche la possibilità (per l'Autorità) di vietare il trattamento nel caso in cui lo stesso sia troppo rischioso, è lecito domandarsi se possa ritenersi esonerato da qualsiasi responsabilità, che non sia quella di mero inadempimento nei confronti del titolare. A causa di tale inadempimento, infatti, i soggetti interessati non potrebbero godere della più ampia tutela loro spettante, che, invece, sarebbe garantita proprio dall'intervento dell'Autorità pubblica.

Ciò che si vuole sostenere è che, nei casi in esame, le situazioni in capo agli interessati appaiono ancora più rilevanti di quella dell'interesse (privato del titolare) a che il DPO adempia diligentemente ai propri doveri per non incorrere in eventuali sanzioni amministrative o in responsabilità nei confronti degli stessi interessati; peraltro, in condizioni normali, vale a dire in caso di operato diligente del DPO, tali situazioni degli interessati verrebbero garantite dall'intervento preventivo dell'Autorità pubblica.

Probabilmente, al fine di superare tali criticità, sarebbe stato opportuno prevedere a monte un obbligo di consultazione preventiva dell'Autorità al termine del D.P.I.A., ovvero un obbligo di notifica del *data breach*, in ipotesi specifiche.

Una previsione di questo tipo sembra poter costituire, infatti, l'unica soluzione possibile al fine di prevenire i fenomeni di cui sopra e salvaguardare l'interesse dei soggetti interessati.

Del resto, altre soluzioni non sembrano essere percorribili, vale a dire, ad esempio, una modifica normativa finalizzata a sgravare il titolare da responsabilità nei confronti dei soggetti lesi al ricorrere delle circostanze di cui sopra, o l'introduzione di eventuali sanzioni dirette nei confronti del DPO da parte dell'Autorità.

Dunque, al ricorrere delle suddette circostanze, sarà pur sempre il titolare a dover rispondere del proprio operato, anche quando questi sia stato a sua volta condizionato dall'operato negligente del DPO, poiché, come sostenuto da una parte della dottrina, l'assenza di colpa del primo nella causazione dell'evento, per aver egli posto in essere l'azione in esecuzione delle istruzioni ricevute dal secondo, non può tradursi in causa di liberazione dalla responsabilità, potendo rintracciarsi una responsabilità per *culpa in eligendo* del DPO[379]. Ci si potrebbe, tuttavia, interrogare sulla possibilità per il titolare di andare esente da eventuali sanzioni di carattere meramente amministrativo, qualora non si sia verificato alcun danno nei confronti di soggetti terzi, ma l'Autorità abbia comunque riscontrato, in seguito ad accertamento successivo, la violazione degli obblighi di cui si è detto.

A sua volta, il DPO non può essere destinatario di un provvedimento di carattere sanzionatorio da parte dell'Autorità, potendo tutt'al più essere destinatario di un'azione diretta da parte dei soggetti lesi, sebbene sia difficile, per i motivi che si vedranno, poter ipotizzare che questi decidano di agire direttamente contro di lui.

Una soluzione che attenuerebbe in parte tale problema potrebbe poi essere, anche alla luce delle riflessioni svolte in merito alle qualità professionali del DPO, quella di introdurre dei meccanismi di certificazione obbligatoria: se, come più volte sottolineato, la figura del DPO serve a garantire una "presenza mediata" del

[379] C. SOLINAS, op. cit., p. 915.

pubblico nel privato, non solo in punto di garanzia a che l'operato del titolare sia conforme al dettato legislativo (funzione, questa, che così interpretata non consentirebbe di cogliere una distinzione effettiva tra il ruolo del DPO e quello degli altri organi di garanzia previsti negli altri settori di riferimento), ma anche nel senso secondo cui è sul DPO che verrebbe a gravare la possibilità o meno per l'Autorità pubblica di intervenire immediatamente in quei settori caratterizzati da un elevato rischio per i diritti e le libertà dei singoli, l'introduzione di un sistema di certificazione, basato, ad esempio, sull'obbligatoria frequenza di corsi professionali (erogati su autorizzazione/accreditamento dell'Autorità garante o da Università Statali) che mirino a offrire al DPO le competenze necessarie per il settore in cui questi si trovi ad operare, garantirebbe l'adeguata formazione professionale di quest'ultimo. L'eventuale negligenza, imprudenza o imperizia, per lo meno, non sarebbero condizionate dal mancato possesso delle competenze adeguate a svolgere un incarico che richiede una professionalità oltremodo avanzata e specialistica, che non è detto possano avere coloro i quali vengono nominati sulla base del titolo di studi di stampo giuridico, o, nei migliori casi, sulla frequenza di corsi generici, ovvero ancora in virtù di esperienze maturate, ma magari non nel settore per il quale si trovano poi ad operare. Rimettendo la scelta del candidato alla posizione di DPO al titolare ed al responsabile, infatti, ben potrebbe accadere che questi si trovi finanche "costretto" a dover nominare un soggetto che possiede delle competenze generali, ma non specialistiche, con riferimento al settore per il quale questi è richiesto, perché magari vi sono pochi candidati alla posizione.

È chiaro che la soluzione paventata, pur non risolvendo del tutto il problema, possa tuttavia tentare di arginarlo.

Altra soluzione, più azzardata, potrebbe essere quella dell'istituzione, da parte del legislatore, di un albo professionale dei DPO, tenuto e gestito dall'Autorità Garante e con accesso vincolato al superamento di una prova abilitativa di carattere nazionale. In primo luogo, l'iscrizione all'albo previo superamento dell'esame consentirebbe di risolvere quanto evidenziato prima con riferimento alla necessità di una certificazione. Ma, soprattutto, l'iscrizione all'albo, previo superamento dell'esame abilitativo, e dunque il riconoscimento ufficiale della

figura in esame, offrirebbe delle garanzie più accentuate a tutti i soggetti che gravitano nel sistema della protezione dei dati personali, dunque non solo al DPO, ma anche ai titolari, ai responsabili ed agli interessati. Il DPO, infatti, sarebbe più solerte nell'adempimento dei propri compiti, stante il rischio di incorrere non solo in un'ipotesi di responsabilità contrattuale nei confronti del titolare, ma altresì in una responsabilità di carattere disciplinare, potendo l'Autorità comminare delle sanzioni quali, a titolo esemplificativo, la sospensione dall'albo, o la revoca nei casi più gravi.

3.1.4 L'obbligo di cooperazione nei casi di condotta colpevole del titolare del trattamento

L'obbligo di cooperazione conduce ad ulteriori interrogativi, che esulano dai casi esaminati in precedenza di condotta colpevole del DPO nella sua attività consulenziale nei confronti del Titolare.

Si vuol fare riferimento a tutte quelle ipotesi, cui si è già fatto un breve cenno con riferimento ai casi di D.P.I.A. e *data breach*, in cui il DPO consigli al titolare di agire in un determinato modo, ma questi non si attenga alle disposizioni indicate (non conformando quindi la propria attività alle indicazioni conformi ai dettami di legge) e, ancora più estensivamente, a tutti quei casi in cui il DPO dovesse riscontrare una violazione della normativa in materia di protezione dei dati personali da parte del titolare.

Si è già fatto cenno all'assenza, in capo al DPO, di poteri di intervento o anche latamente sanzionatori nei confronti del titolare, sottolineando come tale previsione non solo escluda la possibilità di configurare il ruolo del DPO alla stregua di ruolo avente rilievo pubblicistico, ma che altresì non consenta allo stesso DPO di poter obbligare il titolare a conformarsi a quanto da lui suggerito. La *ratio* della mancanza di una tale previsione, peraltro, viene generalmente ricondotta alla considerazione che appare interesse del titolare decidere di conformarsi a quanto indicato dal DPO, ed al contempo è sua assunzione di rischio valutare di non conformarvisi, andando incontro alle eventuali sanzioni.

Tuttavia ci si chiede se, in ragione dell'obbligo di cooperazione con l'Autorità di controllo, e della circostanza per cui, come anticipato, la legge non offre delle

coordinate specifiche in merito al contenuto dello stesso, il DPO non potrebbe essere ritenuto legittimato a poter segnalare o, in via subordinata (nel caso in cui l'Autorità sia già venuta a conoscenza dell'illecito e chieda delle informazioni al DPO) a fornire le informazioni da questa richieste, nonostante l'obbligo di segretezza che grava su questi ai sensi dell'art. 38, par. 5.

Tale obbligo di segnalazione, infatti, consentirebbe una tutela degli interessati particolarmente elevata, com'è facile intuire, specialmente in tutte quelle ipotesi in cui, ad esempio, questi si accorga di ripetute violazioni del GDPR da parte del titolare (con particolare riferimento ai casi in cui tali violazioni pongano in serio pericolo i diritti e le libertà fondamentali degli interessati).

A tal fine, sembrerebbe inoltre necessario porre in essere una distinzione tra settore privato e settore pubblico. Se, infatti, sul DPO che operi in ambito privato, sia in qualità di dipendente sia in qualità di consulente esterno, non sembra potersi fare gravare un obbligo in tal senso, in quanto in possibile conflitto con il generale obbligo di fedeltà e segretezza nei confronti del datore di lavoro, al contrario, sul DPO operante in ambito pubblico, a maggior ragione se già dipendente dell'ente, dovrebbe forse ritenersi sussistente un obbligo di tale portata, stante il generale dovere di collaborazione nei confronti di altre pubbliche amministrazioni di cui all'art. 3, c. 6, d.P.R. 62/2013, cui sono sottoposti tutti i dipendenti pubblici[380].

Alla luce delle riflessioni svolte, sembra potersi ritenere auspicabile, se non necessario, un ripensamento della disciplina inerente il rapporto tra DPO e Autorità, per lo meno nei casi in cui il DPO sia nominato da un soggetto pubblico, ed in particolar modo nei casi in cui ad essere incaricato sia un soggetto già dipendente dello stesso.

In tal senso, si potrebbe forse azzardare un richiamo alla disciplina normativa nazionale dettata in materia di anticorruzione. Si è detto che, ai sensi di tale normativa, sono stati introdotti degli organismi di carattere innovativo a presidio del sistema costruito ai fini di prevenire i fenomeni di corruzione. Accanto

[380] Cfr. M. IASELLI, *Sanzioni e responsabilità in ambito GDPR*, Giuffrè, Collana "*Compliance. Privacy*", luglio 2019, pp. 126 ss. L'Autore, nelle pagine indicate, limita l'oggetto dell'indagine all'obbligo di segretezza del DPO, non anche a quello di segnalazione, il quale, tuttavia, si ritiene possa essere assimilato a quello di segretezza, con riferimento al settore pubblico.

all'Autorità di controllo pubblica (ANAC), è stata altresì istituita la figura del Responsabile della prevenzione della corruzione (RPCT). Il RPCT è una persona fisica, individuata dagli organi di indirizzo delle amministrazioni e dai soggetti tenuti al rispetto delle norme in materia di prevenzione della corruzione, titolare di compiti stabiliti dalla legge e dalle indicazioni programmatiche dell'ANAC, a cui viene affidato il compito di gestire, coordinare e vigilare sulle "*misure*" di prevenzione del rischio corruttivo. Tali funzioni, già a primo impatto, richiamano quelle del DPO, nonché quelle dell'OdV, caratterizzandosi anch'esso per il suo ruolo di "vigilante" e "garante" del sistema. Tuttavia, ciò che, tra l'altro, contraddistingue la prima figura rispetto alle altre due sono i poteri di intervento che gli vengono riconosciuti, anche a carattere sanzionatorio, nei confronti dell'amministrazione in cui opera, che si rivelano necessari al fine di poter meglio garantire il modello di tutela pensato dalla legge, consentendogli di agire in maniera concreta per ridurre i fenomeni di cattiva amministrazione. Ma vi è di più. Al RPCT, infatti, viene riconosciuto altresì un obbligo di segnalazione, tra gli altri, anche nei confronti dell'ANAC, ai sensi dell'art. 43, d. lgs 33/2013 (nei casi in cui l'amministrazione sia inadempiente rispetto agli obblighi di pubblicazione previsti dalla normativa vigente) e ai sensi dell'art 15, d. lgs. 39/2013 (nei casi di possibile violazione delle disposizioni del richiamato decreto).

Come già anticipato, l'introduzione di un obbligo di questo tipo, quanto meno nell'ambito delle realtà pubbliche, anche in considerazione del significato che la cooperazione con il Garante sembra avere, potrebbe essere considerato un apporto migliorativo per il sistema di protezione dei dati, soprattutto in queste realtà.

Inoltre, è il caso di evidenziare che una ipotesi di questo tipo non è completamente avulsa neanche rispetto al sistema di controlli interni tipici delle società private. Basti richiamare quanto già rilevato con riferimento all'OdV, rispetto al quale la disciplina in materia di antiriciclaggio ha introdotto, appunto, l'obbligo di segnalazione nei confronti dell'Autorità pubblica. Ciò ad ulteriore sostegno della tesi per cui, in settori particolarmente esposti a rischio, la possibilità di salvaguardare l'interesse pubblico attraverso l'intervento a carattere "preventivo" di un'Autorità istituita al precipuo fine di un'efficace tutela dello stesso, può rivelarsi decisivo.

4. Riflessi in punto di responsabilità

La scelta di analizzare alcuni esempi pratici in cui, a parere di chi scrive, viene a sostanziarsi l'attività del DPO con riferimento all'obbligo di cooperazione con il Garante, si è resa necessaria al fine di poter trarre ulteriori elementi utili alla definizione della natura giuridica di tale incarico/ufficio, che, come si è visto, non è assimilabile a nessuno di quelli già noti, almeno nel nostro ordinamento nazionale, allorché l'obbligo di cooperazione si traduca nel senso che si è tentato di spiegare nei precedenti paragrafi.

Sebbene, infatti, il DPO sia un organo avente una precipua funzione interna all'azienda, di carattere preminentemente di consulenza e di vigilanza sulla conformità dell'operato del titolare ai princìpi di legge, non può certo non rilevarsi come, in virtù di tale obbligo di cooperazione con l'Autorità, inteso nel senso proposto, lo stesso paia rivestire un ruolo di rilievo non tanto e non solo privatistico, ma quasi, si oserebbe sostenere, "para-pubblicistico", agendo in qualità di referente della stessa Autorità, la quale in tal modo si assicura, all'interno degli enti pubblici e delle aziende, la presenza di un soggetto con il quale condivide il fine ultimo e fondamentale di tutelare la protezione dei dati personali degli interessati. Si assiste, in sostanza, ad una sorta di "privatizzazione" della stessa Autorità di controllo, cui il DPO si sostituisce nell'ambito delle realtà ove deve essere nominato, presentandosi come un Garante "personale" o di "Garante in casa", chiamato a tutelare l'interesse dei soggetti interessati, in via preventiva rispetto all'Autorità pubblica.

Non è un caso che molti DPO abbiano sostenuto, nel corso dei dibattiti che in questi anni si sono succeduti, tanto nelle sedi universitarie quanto nell'ambito dei corsi di formazione organizzati da società private, che la sensazione avvertita dai titolari è che spesso il DPO sia più un "ispettore", che un consulente "dalla parte" del titolare. Così, tuttavia, non deve essere: il DPO riveste pur sempre il ruolo principale di consulente, sebbene egli debba agire secondo canoni di diligenza volti non solo ad adempiere nel migliore dei modi la propria prestazione a salvaguardia dell'interesse del titolare, ma, principalmente, orientando il suo operato nell'ottica della migliore tutela possibile dell'interesse pubblico. A sostegno di tale assunto, basti considerare la necessità che il DPO sia scelto in

virtù delle proprie competenze professionali, di carattere altamente specialistico, sebbene, come si è già avuto modo di rilevare, proprio in virtù della natura dell'incarico e delle finalità perseguite attraverso l'introduzione di detta figura nell'ambito di determinate realtà, sarebbe forse stato più utile introdurre un obbligo di certificazione della professione in esame.

Nonostante tutte le considerazioni svolte, non si può tuttavia prescindere dal dato testuale, che non offre alcun margine utile al fine di poter ascrivere tale ruolo entro la categoria dei ruoli aventi rilievo pubblicistico. Infatti, come si è già evidenziato, esattamente come avviene per l'OdV, il legislatore non ha previsto in capo al DPO dei poteri di intervento o impeditivi da esercitare nei confronti del titolare, nonostante la posizione di garanzia che questi riveste, né prevede un obbligo di segnalazione nei confronti dell'Autorità di controllo di eventuali condotte illecite riscontrate.

Ciò costituisce di per sé un chiaro indice della volontà di attribuire a tale soggetto un rilievo meramente endo-organizzativo. Il DPO si presenta, dunque, come un "ufficio interno" della società o dell'ente, il cui operato non ha dirette conseguenze esterne: non a caso, nessuna norma richiede una pubblicità esterna alle risultanze del suo operato. Ciò solo basterebbe ad escludere una responsabilità extracontrattuale nei confronti di eventuali interessati e soggetti terzi lesi dal trattamento. Del resto, il GDPR prevede, agli artt. 82 e 83, che la responsabilità per violazione della legge vada fatta gravare esclusivamente sul titolare del trattamento (e sul responsabile, nei casi previsti), unico destinatario delle sanzioni amministrative irrogate dall'Autorità, nonché dell'obbligo del risarcimento dei danni derivati.

Il DPO, invece, non è destinatario di una specifica responsabilità ad effetto esterno. Si tratta di uno statuto speciale del DPO "che si evidenzia per il fatto che risulta pure sottratto al principio di responsabilità solidale stabilito dal GDPR tra più Titolari e Responsabili"[381].

Tuttavia, come evidenziato da autorevole dottrina, sebbene non sia oggetto di specifica disciplina, la responsabilità del DPO non costituisce nemmeno oggetto di espressa esclusione dal dettato legislativo: non pare dunque potersi escludere

[381] E. TOSI, *La responsabilità civile per trattamento illecito dei dati personali*, in E. TOSI (a cura di), op. cit., p. 662.

del tutto la possibilità di un'eventuale azione diretta da parte del danneggiato per illecito trattamento dei dati personali, sebbene tale azione non potrà beneficiare del regime speciale di cui all'art. 82 GDPR, riservato alle azioni di responsabilità civile nei confronti del titolare e del responsabile, ma dovrà seguire le regoli comuni del codice civile.

In questo senso, dovrà farsi riferimento all'art. 2043 c.c., in ragione del quale il danneggiante dovrà provare il dolo o la colpa grave del DPO nella causazione del fatto dannoso e del danno subito[382]. In particolare, tale azione si potrebbe configurare, ad esempio, proprio in tutte quelle ipotesi in cui egli abbia agito in modo colpevole, determinando il titolare ad agire in violazione delle norme del GDPR.

Stante quanto sopra, resta in ogni caso fermo il principio per cui il DPO sarà pur sempre tenuto a rispondere nei confronti del titolare o del responsabile per l'inadempimento dei propri doveri, in virtù del rapporto contrattuale che lo lega a questi, nel caso in cui l'azione di risarcimento danni nei loro confronti, o l'irrogazione di sanzioni, sia stata causata dalla sua condotta negligente.

In tal caso, l'onere della prova relativamente all'inadempimento da parte del DPO degli obblighi contrattuali graverà sul titolare del trattamento. Se questi riuscirà a fornire la prova, sul DPO graverà a sua volta l'onere di provare che l'inadempimento è stato determinato da causa a lui non imputabile, e dunque di essere esente da colpa, o meglio da colpa grave, in considerazione del fatto che ci troviamo dinanzi a una prestazione d'opera intellettuale. Com'è noto, per "professione intellettuale" si intende una prestazione professionale per il cui adempimento è richiesto l'uso di una particolare "preparazione tecnica", a prescindere dal carattere stabile e continuativo oppure occasionale dell'attività medesima. La professione intellettuale, inoltre, è qualificata dal carattere intellettuale dell'attività svolta, nel senso che l'uso delle facoltà intellettive deve avere un ruolo preminente nell'esplicazione delle prestazioni dedotte in contratto:

[382] E. TOSI, op. cit., p. 663. L'Autore rileva, invero, che "*non si vedono evidenti ragioni per le quali un danneggiato che possa contare sull'ampio concorso patrimoniale di titolari e responsabili – in solido tra loro per l'intero danno subito – debba ritenere opportuno citare in giudizio direttamente anche il DPO e affrontare il più gravoso onere probatorio ordinario in assenza di inversione dell'onere della prova prevista, si ribadisce, esclusivamente per i Titolari e i Responsabili*".

in tal senso, il criterio della tecnicità e quello dell'intellettualità sono strettamente correlati, ed entrambi strumentali all'esercizio della professione[383]. Dalla qualificazione di un'attività come intellettuale dipende l'applicazione dell'art. 2236 c.c., il quale prevede che, se la prestazione implica la soluzione di problemi tecnici di speciale difficoltà, il prestatore d'opera non risponde dei danni, se non in caso, appunto, di dolo o colpa grave[384].

5. Considerazioni conclusive

Al termine delle considerazioni svolte, emerge come non sia possibile, allo stato attuale, poter fornire un quadro regolamentare completo ed esaustivo in merito a questa nuova, importante, figura introdotta dal GDPR, in considerazione sia della genericità delle disposizioni normative che della carenza di specificazioni ed interventi del legislatore nazionale.

Il GDPR , infatti, pur avendo dedicato tre norme alla disciplina del ruolo in esame, ha mancato di fornire indicazioni dettagliate sia sull'effettiva estensione dell'ambito dei poteri dello stesso sia sulle caratteristiche specifiche che devono appartenere a tale figura, limitandosi a prevedere che questi deve essere scelto in virtù delle sue "qualità professionali" (termine che si presta già di per sé a dover

[383] Cfr. G. FACCI, *La responsabilità civile del professionista*, Cedam, 2006, pp. 1-2. Altri caratteri, anche se non esclusivi, delle prestazioni svolte dal professionista intellettuale sono la discrezionalità e la personalità: la discrezionalità indica la facoltà di scelta che il professionista ha sul comportamento da tenere e sui mezzi tecnici da adottare nell'esercizio delle sue funzioni, mentre il carattere della personalità insiste sulla necessità che il prestatore esegua personalmente l'incarico assunto, potendo avvalersi di sostituti ed ausiliari solo entro certi limiti. È chiaro che, con riferimento all'incarico di DPO, la discrezionalità si sposa con la necessità che allo stesso venga garantita autonomia ed indipendenza rispetto al Titolare, anche nei casi in cui ad essere nominato sia un soggetto già dipendente dell'ente. La personalità, invece, come si è visto, viene garantita dalla previsione in virtù della quale, anche nel caso in cui ad essere nominata sia una persona giuridica, è necessario vengano indicati i dati di contatto di un unico DPO, rispetto al quale gli altri dipendenti della società fungeranno eventualmente da ausiliari.

[384] Il testo della norma, così come la Relazione del ministro Guardasigilli (n. 917) sembrano introdurre un criterio di attenuazione della responsabilità del professionista, nella parte in cui si prevede la limitazione della responsabilità al dolo e alla colpa grave, in caso di prestazioni che implicano la soluzione di problemi tecnici di speciale difficoltà. Nella relazione, in particolare, si afferma la volontà del legislatore di contemperare due opposte esigenze, quella di non mortificare l'iniziativa del professionista con il timore di ingiuste rappresaglie da parte del cliente in caso di insuccesso o riprovevoli inerzie del professionista, e quella contraria di non indulgere verso non ponderate decisioni o riprovevoli inerzie del professionista. L'art. 2236 cc si riferisce, come visto, ai "problemi tecnici", pertanto la colpa che viene in rilievo è quella per aver agito con imperizia, vale a dire in violazione di regole tecniche e in mancanza di determinate cognizioni; invece, nella diversa ipotesi in cui la responsabilità trovi la propria origine nella negligenza o nell'imprudenza, il professionista risponde secondo le regole comuni (art. 1176, c. 2), con la conseguenza che è rilevante anche la colpa lieve. Cfr. G. FACCI, op. cit., pp. 16-19.

essere riempito di significato), ed in particolare delle sue "conoscenze specialistiche sulla normativa", senza però porre l'accento sulla necessità, oltremodo evidente, che il DPO abbia, altresì, conoscenze giuridiche specifiche in relazione alla realtà in cui sarà tenuto ad operare, ed ulteriormente conoscenze di carattere tecnico.

Anche le norme dedicate al rapporto (di lavoro) intercorrente tra DPO e titolare si presentano oltremodo generiche e astratte, poiché il legislatore si limita a sancire, da un lato, che il rapporto deve essere regolato tra le parti a mezzo di una lettera di incarico (se il DPO è già dipendente dell'ente) o a mezzo di un contratto di servizi (se è invece esterno) e, dall'altro, che il DPO non possa subire ritorsioni per lo svolgimento del proprio incarico, senza specificare però come si debba comportare il titolare nel caso in cui il DPO non adempia, o non adempia diligentemente, il proprio incarico, e senza offrire una garanzia più pregnante allo stesso DPO per il caso in cui il titolare non rispetti tale divieto, ponendo in essere condotte discriminatorie nei suoi confronti.

Viene così lasciato aperto il campo a diverse possibili soluzioni, che si è tentato di passare in rassegna. Con riferimento al primo punto, inerente i poteri del DPO, si è già detto che gli stessi possono essere distinti, da un lato, in poteri di consulenza e vigilanza nei confronti del titolare, e, dall'altro, in poteri di cooperazione con l'Autorità. Dai primi due poteri, si è visto, discende l'onere per il DPO di collaborare attivamente con il titolare al fine di garantire la massima implementazione possibile del sistema di protezione dei dati personali, e al tempo stesso vigilare sulla concreta osservanza dei princìpi legislativi, poiché, come si è più volte evidenziato, il DPO ha solo funzioni di carattere consultivo, mentre la concreta attuazione delle misure eventualmente proposte spetterà pur sempre al titolare: il DPO, infatti, non gode di poteri di intervento diretto, di carattere coercitivo o sanzionatorio o impeditivo dell'azione, ma solo di poteri di indagine, che danno luogo a risultanze di carattere esclusivamente interno. Tuttavia, come si è sottolineato, l'obbligo di cooperazione con l'Autorità fa sorgere il dubbio circa la necessità di una modifica della disciplina in tal senso, attraverso l'introduzione, ad esempio, di un potere di segnalazione di eventuali condotte illecite o semplicemente non conformi ai pareri resi, specie in tutti quei casi in cui il DPO

operi nell'ambito di un ente pubblico, e dunque sia chiamato a garantire un interesse di rilievo pubblico. In generale, poi, si è altresì visto come potenziare il ruolo dell'Autorità nell'ambito del rapporto di lavoro intercorrente tra titolare e DPO potrebbe rivelarsi una scelta efficace anche al fine di garantire meglio la posizione di indipendenza di quest'ultimo.

Con riferimento, invece, alle caratteristiche proprie della figura, si è già detto come sia oltremodo pacifico che questi debba essere autonomo ed indipendente rispetto al titolare e responsabile, sia nel caso in cui venga nominato un soggetto esterno sia nel caso in cui invece si tratti di soggetto già dipendente dell'ente. A tal riguardo, la legge non esprime preferenza per l'una o l'altra alternativa, sebbene, come si è rilevato, la scelta di un soggetto esterno, persona fisica, sembra essere quella migliore, fatta salva la possibilità poi per il DPO di avvalersi, all'interno dell'ente, di un *team* di persone che, con il loro ausilio, consentirebbero l'efficacia dell'azione di quest'ultimo. Contrariamente, l'incarico assegnato a una persona giuridica, e non fisica, se auspicabile in considerazione della possibilità di avvalersi di professionalità di diverso tipo, fatta salva in ogni caso la necessità che venga individuata una persona specifica, tra i dipendenti della società incaricata, che funga da punto di contatto con il titolare, potrebbe, tuttavia, dar luogo ad aspetti problematici di particolare rilievo con riferimento alla regolazione del rapporto di lavoro, tanto tra titolare e società incaricata, quanto tra quest'ultima e il soggetto indicato per svolgere l'incarico.

Ancora, sempre con riferimento ai requisiti della figura in esame, deve evidenziarsi come sia alquanto controverso determinare con esattezza gli stessi. Infatti, il DPO deve essere scelto tenendo concretamente conto della quantità ed eventuale eterogeneità dei trattamenti posti in essere. In particolare, la legge puntualizza la necessità che questi abbia una conoscenza specialistica della normativa in materia di protezione dei dati personali, tuttavia è oltremodo evidente come egli debba avere anche un'approfondita conoscenza delle fonti normative che vengono in rilievo nello specifico settore in cui il titolare opera, nonché delle principali problematiche inerenti lo stesso, e che allo stesso tempo abbia delle conoscenze tecniche di rilievo. Si tratta di qualità che non è detto che ogni DPO candidato alla posizione possegga, specie nel caso in cui questi venga

scelto tra i dipendenti interni, ipotesi frequente dato il risparmio di *budget* che ne deriva. Al riguardo ci si è chiesti se, anche alla luce dell'obbligo di cooperazione di cui si è detto, da interpretarsi nel senso di possibilità che, in caso di operato colpevole del DPO, questi possa condizionare l'intervento preventivo dell'Autorità in tutti i casi di trattamenti particolarmente rischiosi, non sarebbe stato forse più opportuno introdurre un obbligo di certificazione che, offrendo al DPO la possibilità di essere adeguatamente formato in relazione al compito da svolgere, renderebbe il suo operato meno esposto a possibili condotte colpevoli, oppure ancora, la possibilità di introdurre l'istituzione di un albo di DPO gestito direttamente dall'Autorità.

Così sommariamente ripresi i punti salienti dell'analisi condotta, appare con ogni evidenza come ci si trovi dinanzi ad un ruolo unico nel suo genere, dotato di peculiarità che lo rendono non assimilabile a nessuna delle altre figure più note nell'ambito del sistema dei controlli interni alla società o all'ente pubblico, con particolare riferimento a quelle, più rappresentative, dell'OdV e del RPCT, di cui tuttavia sembra compendiare le funzioni, rappresentando, in maniera evidente, una evoluzione di queste ultime.

La natura ibrida dello stesso viene resa poi ancor più evidente dalla circostanza per cui è obbligatorio che questi sia presente tanto nel settore pubblico quanto in quello privato, entrambi destinatari della medesima disciplina normativa, nonostante la evidente necessità di dedicare norme diverse per settori che richiedono una regolamentazione diversa.

Alla luce di tutto quanto sopra, sembra naturale porsi l'interrogativo circa la necessità o meno di un ripensamento della disciplina inerente il ruolo oggetto di indagine, attraverso l'introduzione di previsioni che diano una fisionomia più precisa alla funzione del DPO complessivamente intesa.

Tale funzione, infatti, a tutti gli effetti costituisce il vero "fulcro" del sistema di protezione dei dati personali, ed una maggiore specificazione di funzioni e responsabilità risulterebbe certamente più funzionale all'interesse che il DPO è chiamato a garantire, che è quello della protezione dei dati personali degli interessati, oltre che quello, individuale, del titolare del trattamento (sebbene il primo possa essere garantito anche in ragione della tutela del secondo).

Si è infatti già avuto modo di evidenziare, più volte, come tale ruolo sia stato previsto come obbligatorio proprio in tutte quelle realtà in cui il trattamento presenti un elevato grado di rischiosità per il diritto alla protezione dei dati personali e le libertà fondamentali degli individui. Ciò rende necessario che il titolare, al fine di garantire la migliore tutela possibile ai soggetti interessati, venga coadiuvato da un soggetto altamente specializzato, il quale si presenta come garante, dinanzi all'Autorità e agli stessi interessati, della conformità dell'operato dello stesso alla legge. Il fatto che manchino dei poteri più incisivi da esercitare nei confronti del titolare, sebbene conduca alla conclusione che l'interesse protetto sia quello privato di quest'ultimo, tuttavia non deve portare a escludere *a priori* la possibilità che con il tempo questi inizi ad assumere un rilievo anche pubblicistico. La stessa nomenclatura del ruolo, d'altronde, suggerisce come non sia possibile pensare al DPO come ad un mero organo di vigilanza, dal momento che questi è "responsabile della protezione dei dati personali" e proprio da tale responsabilità discendono tutte le riflessioni critiche in merito alla genericità delle norme dedicate all'incarico, con particolare riferimento, peraltro, proprio all'obbligo di cooperazione, di cui tanto si è discusso. Una rivisitazione, o meglio, una precisazione di alcuni punti della disciplina normativa inerente tale incarico, avrebbe esclusivamente il pregio di potenziarne le caratteristiche, nell'ottica di una maggior garanzia del diritto alla protezione dei dati personali, fulcro e motore dell'intera disciplina, la quale ha delineato a tal fine un sistema di cui il DPO costituisce strumento elettivo ai fini di un ottimale funzionamento.

INDICE BIBLIOGRAFICO

- R. ACCIAI, *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice*, Maggioli, Santarcangelo di Romagna, 2004

- G. AIELLO, *La protezione dei dati personali dopo il Trattato di Lisbona*, in *Oss. del dir. civ. e comm.*, n. 2/2015

- G. ALPA, *Raccolta di informazioni, protezione dei dati e controllo degli elaboratori elettronici (in margine ad un progetto di convenzione del Consiglio d'Europa)*, in *Foro.it*, 1981, 2, pt. V

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

- G. ALPA, *I diritti della personalità*, in G. ALPA – G. RESTA, *Le persone e la famiglia. 1) Le persone fisiche e i diritti della personalità*, in R. SACCO, *Trattato di diritto civile*, Giappichelli, Torino, 2006

- M. ALTMAN, A. WOOD, D. R. O'BRIEN, U. GASSER, *Practical approaches to Big Data privacy over time, International Data Privacy Law*, 2018, Vol. 8, N. 1

- G. AMATO, *Autorità semi-indipendenti ed autorità di garanzia*, in *Riv. Trim. di diritto pubblico*, 1997

- T. AMEDEO AULETTA, *Riservatezza e tutela della personalità*, Giuffrè, Milano, 1978

- G. ARCELLA, *GDPR: il Registro delle attività di trattamento e le misure di accountability*, in *Rivista di Notariato*, 4/2018

- L. ARCIDIACONO, *Governo, Autorità indipendenti e pubblica amministrazione*, in S. LABRIOLA (a cura di), *Le autorità indipendenti*, Giuffrè, Milano, 1999
- M. ATELLI – M. MAZZEO, *Le definizioni del Codice dei dati personali*, in V. CUFFARO R. D'ORAZIO – V. RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, Giappichelli, Torino, 2007

- A. AVITABILE, *Il Data Protection Officer*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017

- V. BAGNOLI, *The Big Data relevant market*, in *Concorrenza e mercato*, 23, 2016

- A. BALDASSARRE, *Privacy e Costituzione. L'esperienza statunitense*, Roma, 1974

- F. BALDUCCI ROMANO, *La protezione dei dati personali nell'Unione europea tra libertà di circolazione e diritti fondamentali dell'uomo*, in *Rivista italiana di diritto pubblico comunitario*, 2015

- P. BASTIA*, I modelli organizzativi*, in AA. VV., *Reati e responsabilità degli enti*, Milano, 2005

- A. BAUDINO – C. SANTORIELLO, *La responsabilità dei componenti dell'Organismo di Vigilanza*, in *Resp. Amm. Enti*, 2009, II

- G. BELLOMO, *Contributo alla problematica della natura giuridica del "Data Protection Officer" (DPO)*, 26 marzo 2020, rinvenibile al *link* *http://www.giurcost.org/LIBERAMICORUM/bellomo_scrittiCostanzo.pdf*

- A. BELVEDERE, *Riservatezza e strumenti d'informazione*, in N. IRTI (a cura di), *Dizionari di diritto privato*, vol. 1, Diritto civile, Giuffrè, Milano, 1980

- N. BERNARDI, *Il Garante per la privacy bavarese si prepara a sparare sulla Croce Rossa*, rinvenibile al link *https://nicolabernardi.nova100.ilsole24ore.com/2019/08/31/il-garante-privacy-bavarese-pronto-a-sparare-sulla-croce-rossa/*

- M. BIANCA – F. BUSNELLI (a cura di*), La protezione dei dati personali*, Cedam, Milano, 2007

- R. BIFULCO – M. CARTABIA – A. CELOTTO, *L'Europa dei diritti*, Il Mulino, Bologna, 2001

- F. BIGNAMI, *Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network*, in *Michigan Journal of International Law*, 2005, vol. 26

- F. BIGNAMI, *Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy*, 59 AM. J. COMP. L. 411, (2011)

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

- F. BOEHM, *Information sharing and data protection in the Area of Freedom, Security and Justice*, Springer, Berlin, 2012

- L. BOLOGNINI - C. BISTOLFI, *Pseudonymization and Impacts of Big (Personal/Anonymous) Data Processing in the Transition from the Directive 95/46/EC to the New EU General Data Protection Regulatio*n, in *Computer Law & Security Review*, 2017

- A. BONFANTI*, L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta La giurisprudenza della Corte di giustizia in materia di digital privacy come osservatorio privilegiato*, in *Medialaws*, 3/2018

- S. BOURDILLON-KNIGHT, *Anonymous data v. personal data-a false debate: an EU perspective on anonymization, pseudonymization and personal data*", in *Wisconsin International Law Journal*, n. 2/2016

- F. BRAVO, *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tramercato e persona: nuovi assetti nell'ordinamento europeo?*, in *Contratto e impresa*, 1/2018

- F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Le monografie di Contratto e impresa, Cedam, Milano, 2018

- A. BRECCIA, *Riconoscimento e politica dei diritti umani sul piano europeo e internazionale*, in L. PANELLA (a cura di), *I diritti umani nella giurisprudenza e nella prassi del diritto internazionale ed europeo*, Giappichelli, Torino, 2013

- R. BRIGHI, *Il ruolo dei dati informatici nella costruzione della realtà*, Aracne, Roma, 2016

- N. BRUTTI, *Le figure soggettive delineate dal GDPR: la novità del Data Protection Officer*, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè, Milano, 2019

- A. BUSACCA, *Il diritto di accesso ad Internet*, in *Ordine internazionale e diritti umani*, 2017, pp. 345-359, rinvenibile al *link* *http://www.rivistaoidu.net/content/%E2%80%9Cdiritto-di-accesso%E2%80%9D-alla-rete-internet*

- A. BUSACCA, *88. Trattamento dei dati nell'ambito dei rapporti di lavoro*, in G.M. RICCIO - G. SCORZA – E. BELISARIO, *GDPR e Normativa Privacy Commentario*, Wolters Kluver, Milano, 2018

- G. BUSIA, *Il ruolo dell'Autorità Indipendente per la protezione dei dati personali*, in N. ZORZI GARGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Wolters Kluwer Italia, Milano, 2019

- G. BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione*, Giuffrè, Milano, 1997

- G. BUTTI, *Il DPO e il rischio di conflitto di interessi: profili e allocazione delle responsabilità*, 23 aprile 2019, rinvenibile al link *https://www.cybersecurity360.it/legal/privacy-dati-personali/il-dpo-e-il-rischio-di-conflitto-di-interessi-profili-e-allocazione-delle-responsabilita/*

- L. CALIFANO, *Privacy: affermazione e pratica di un diritto fondamentale*, Editoriale scientifica, Napoli, 2016

- L. CALIFANO, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dati personali*, in L. CALIFANO – C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale scientifica, Napoli, 2019

- L. CALIFANO – C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale scientifica, Napoli, 2019

- S. CALZOLAIO, *Protezione dei dati personali*, in «*Dig. Disc. Pubbl.*», Agg., Utet Giuridica Wolters Kluwer, Milano, 2017

- S. CALZOLAIO – L. FEROLA – V. FIORILLO – E. A. ROSSI – M. TIMIANI, *La responsabilità e la sicurezza del trattamento*, in L. CALIFANO – C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale scientifica, Napoli, 2019

- R. CANTONE – E. CARLONI, *La prevenzione della corruzione e la sua Autorità*, in *Diritto pubblico*, 3/2017, Il Mulino

- F. CARDARELLI - S. SICA – V. ZENO ZENCOVICH (a cura di), *Il Codice dei dati personali: temi e problemi*, Giuffrè, Milano, 2004

- F. CARINGELLA, *Le Autorità indipendenti tra neutralità e paragiurisdizionalità*, in *Il Consiglio di Stato*, 2000, 3

- S. CASSESE – C. FRANCHINI (a cura di), *I garanti delle regole*, Il Mulino, Bologna, 1996

- C. CASTRONOVO, *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali*, in V. CUFFARO – V. RICCIUTO – Z. ZENO ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, Giuffrè, Milano, 1999

Centro Studi «Federico Stella» sulla Giustizia penale e la Politica criminale (a cura di), *Esperienze di avvio degli Organismi di Vigilanza* ex *d.lgs. 231/2001*, Quaderno n. 244, 2008

- A. CICCIA MESSINA, *Stop all'incetta di nomine di Data Protection Officer*, rinvenibile al link *https://federprivacy.org/informazione/primo-piano/item/1029-dpo-stop-alla-incetta-di-nomine*

- G. P. CIRILLO, *La tutela della privacy nel sistema del nuovo Codice sulla protezione dei dati personali*, Cedam, Padova, 2004

- G. P. CIRILLO (a cura di), Il c*odice sulla protezione dei dati personali*, Giuffrè, Milano, 2004

- C. COLAPIETRO – A. IANNUZZI, *I princìpi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. CALIFANO – C. COLAPIETRO, *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale scientifica, Napoli, 2019

- G. COMANDE', *Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità*, in *Analisi Giuridica dell'Economia*, Fascicolo 1, giugno 2019

- S. COMELLINI, *Il Responsabile della Protezione dei Dati (Data Protection Officer – DPO)*, in *Soluzioni di Diritto* (direzione scientifica di N. GRAZIANO**)**, Maggioli Editore, 2018

- B. CORTESE, *La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona*, in *Dir. Un. Eur.*, 2013, n. 2

- B. CORTESE, *Art. 16 TFUE*, in A. TIZZANO (a cura di), *Trattati dell'Unione europea*, Giuffrè, Milano, 2013

- V. CUFFARO – V. RICCIUTO (a cura di), *Il trattamento dei dati personali*, *Vol. II, Profili applicativi*, Giappichelli, Torino, 1999

- V. CUFFARIO – R. D'ORAZIO – V. RICCIUTO, *Il codice del trattamento dei dati personali*, Giappichelli, Torino, 2007

- V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali*, *Contratto e impresa*, 3/2018

- V. CUFFARO*, Il diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia: elementi per un bilancio ventennale*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019

- N. DA SILVIA, *Artificial Neural Networks – A Practical Course*, Zurich, 2017

- A. DE CUPIS*, I diritti della personalità*, in F. MESSINEO – L. MENGONI*, Trattato di diritto civile e commerciale*, IV, Giuffrè, Milano, 1982

- A. DE MAURO, *A formal definition of Big Data based on its essential features*, *Library Review*, 2016, vol. 65, n. 3

- G. DE MINICO, *Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria*, in *Dir. Pubb.*, fasc. 1, gennaio-aprile 2019

- G. DE VERO, *La responsabilità penale delle persone giuridiche. Parte generale*, Milano,2008

- G. D'ACQUISTO-M. NALDI, *Big Data e privacy by design*, Giappichelli, Torino, 2017

- G. D'IPPOLITO, *Il principio di limitazione delle finalità del trattamento tra data protection e antitrust. Il caso dell'uso secondario di Big Data*, in *Dir. Inf.*, fasc. 6

- F. D'ARCANGELO*, Il ruolo e la responsabilità dell'Organismo di Vigilanza nella disciplina antiriciclaggio*, in *Resp. Amm. Enti*, 2009, I

- R. D'ORAZIO, *Garante per la protezione dei dati personali*, in E. GIANNANTONIO - M. G. LOSANO - V. ZENO-ZENCOVICH (a cura di), *Il trattamento dei dati personali*, Cedam, Padova, 1999

- V. R. D'ORAZIO, *Protezione dei dati by default e by design*, in S. SICA – V. D'ANTONIO - G. M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, Cedam, Milano, 2016

- R. D'ORAZIO, *La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale*, in V. CUFFARO – R. D'ORAZIO – V. RICCIUTO, *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019

- G. DELLA MORTE, *Big Data e protezione internazionale dei diritti umani*. *Regole e conflitti*, Editoriale Scientifica, Napoli, 2018

- F. DI PORTO (a cura di), *Concorrenza e mercato. Antitrust, Regulation, Consumer Welfare, Intellectual Property - Vol. 23/2016*

- F. DI PORTO, *Big Data e concorrenza*, CeM, n. spec. 23/2016

- M. S. ESPOSITO, *Trattamento dei dati personali e rischi correlati, nel prisma dei diritti e delle libertà fondamentali*, in *Dir. Inf.*, fasc. 4, 2018

- A. ESTEVE, *The business of personal data: Google, Facebook, and privacy issues in the EU and the USA*, *International Data Privacy Law*, 2017, Vol. 7, No. 1

- A. FABBRICOTTI, L. RAPONI, *La struttura multilivello della protezione dei dati personali in Europa*, in *Rivista italiana per le scienze giuridiche*, 8/2017

- G. FACCI, *La responsabilità civile del professionista*, Cedam, 2006

- G. B. FERRI, *Privacy e libertà informatica*, in G. ALPA – M. BESSONE (a cura di), *Banche dati telematiche e diritti della persona*, Cedam, Padova, 1984

- A. FINLAY, R. MADIGAN, *GDPR and the Internet of Things: 5 Things You Need to Know*, rinvenibile al link *www.lexology.com*

- G. FINOCCHIARO, «*Identità personale (diritto alla)*», in *Digesto Civile*, Agg., Utet, Torino, 2010

- G. FINOCCHIARO – F. DELFINI, *Diritto dell'Internet*, Giuffrè, Milano, 2014

- G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli, Bologna, 2016

- G. FINOCCHIARO, *Introduzione al Regolamento europeo sulla protezione dei dati, in «Le Nuove Leggi Civili Commentate»*, 1/2017

- G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017

- G. FINOCCHIARO, *Riflessioni sul poliedrico Regolamento europeo sulla privacy*, in *Quaderni costituzionali*, Fascicolo 4, dicembre 2018

- G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Zanichelli, Bologna, 2019

- A. FIORELLA, voce *Responsabilità da reato degli enti collettivi*, in CASSESE (dir.), *Dizionario di diritto pubblico*, V, Milano, 2006

- V. FROSINI, *Diritto alla riservatezza e calcolatori elettronici*, in G. ALPA – M. BESSONE (a cura di), *Banche dati telematiche e diritti della persona*, Cedam, Padova, 1984

- G. B. GALLUS, *Il DPO deve essere dipendente dell'azienda affidataria dell'incarico": il Tar Lecce fa discutere*, reperibile al link https://www.cybersecurity360.it/news/il-dpo-deve-essere-un-dipendente-non-puo-essere-esterno-il-tar-lecce-fa-discutere/

- G.B. GALLUS – M. PINTUS, *Data protection impact assessment*, in G. CASSANO - V. COLAROCCO, G.B. GALLUS, F.P. MICOZZI (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, Giuffrè, 2018

- M. GAMBINI, *Principio di responsabilità e tutela aquiliana dei dati personali*, *Quaderni della Rassegna di diritto civile diretta da Pietro Perlingieri*, *Edizioni Scientifiche Italiane*, 2018
- A. GANDOMI – M. HAIDER, *Beyond the hype: Big data concepts, methods and analytics*, in *International Journal of Information Management*, 2015, vol. 35

- R. GELLERT, *Understanding the notion of risk in the General Data Protection Regulation*, in *Computer Law and Security Review*, 2018

- G. GIANNONE CODIGLIONE, *Libertà d'impresa, concorrenza e neutralità della Rete nel mercato transnazionale dei dati personali*, in *Dir. Inf.*, 2015

- G. GIANNONE CODIGLIONE, *Risk based approach e trattamento dei dati personali*, in S. SICA – V. D'ANTONIO - G. M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, Cedam, Milano, 2016

- G. GIANNONE CODIGLIONE, *Internet of Things e nuovo Regolamento Privacy*, in S. SICA - V. D'ANTONIO - G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, Cedam, Milano, 2016

- G. GIANNONE CODIGLIONE, *La tutela della riservatezza*, in S. SICA - V. ZENO ZENCOVICH, *Manuale di diritto dell'informazione e della comunicazione*, Cedam, Milano, 2017

- A. GORASSINI, *Lo spazio digitale come oggetto di un diritto reale?*, in *Medialaws*, n. 2/2018,

- M. GRANIERI, *Il trattamento di categorie particolari di dati personali nel reg. UE 2016/679*, in *Le nuove leggi civili commentate*, n. 1/2017

- E. L. GUASTALLA, *Privacy e Data Protection: principi generali*, in E. TOSI (a cura di), E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè, Milano, 2019

- M. IASELLI, *DPO di un ente pubblico: qualifica e requisiti*, 8 novembre 2018, rinvenibile al link *https://www.agendadigitale.eu/sicurezza/privacy/dpo-di-un-ente-pubblico-qualifica-e-requisiti*

- M. IASELLI, *Sanzioni e responsabilità in ambito GDPR*, Giuffrè, Collana "*Compliance. Privacy*", 2019

- ITMEDIA CONSULTING BOCCONI (a cura di), *L'economia dei dati. Tendenze di mercato e prospettive di policy*, Roma, Gennaio 2018, rinvenibile al link: *www.itmedia-consulting.com/it/highlights/1187-leconomia-dei-dati-tendenze-di-mercato-e-prospettive-di-policy-lostudiofondamentale-sui-big-data-2.html*

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

- R. LATTANZI, *«Diritto alla protezione dei dati di carattere personale»: appunti di viaggio*, in AA. VV., *Diritto alla privacy e trattamento automatizzato dei dati fra diritto civile, diritto penale e diritto internazionale ed europeo*, *I quaderni europei*, Aprile 2014, n. 63

- E. LAUCHAD, *DPO certification should be regulated?*,
Maggio 10/2018), reperibile al link *https://ssrn.com/abstract=3176471*, o *http://dx.doi.org/10.2139/ssrn.3176471*

- M. LA ROSA, *Teoria e prassi del controllo interno ed esterno sull'illecito dell'ente collettivo*, in *Riv. it. dir. proc. pen*., 2006

- O. LYNSKEY, *The Foundations of EU Data Protection Law*, Oxford, 2015

- A. MANTELERO, *Il costo della privacy tra valore della persona e ragione d'impresa*, Giuffrè, Milano, 2007

- A. MANTELERO, *La riforma della Data Protection in Europa: un'opportunità per le imprese*, in *Giustiziacivile.com*, approfondimento del 03 marzo 2014

- A. MANTELERO, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Le nuove leggi civili commentate*, Cedam, 1/2017

- A. MANTELERO, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati*, in G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017

- A. MANTELERO, *Regulating Big Data. The guidelines of the Council of Europe in the context of the European data protection framework*, in *Computer Law and Security Review*, 2017

- R. MARTINEZ, *El delegado de protecciòn de datos, in A. RALLO LOMBARTE (a cura di), Tratado de protecciòn de datos: actualizado con la Ley Organicà 3/2018, de 5 de diciembre, de proteccion de datos personales y garantìa de los derechos digitales*, Tirant lo Blanch, 2019

- J. MAZZETTO, *L'audit privacy: i consigli pratici per individuare le criticità nella sicurezza dei dati personali*, rinvenibile al link *https://www.cybersecurity360.it/legal/privacy-dati-personali/laudit-privacy-i-consigli-pratici-per-individuare-le-criticita-nella-sicurezza-dei-dati-personali/.*

- V. MAYER SCHONBERGER – K. CUKIER, *Big Data: A Revolution That Will Transform how We Live, Work, and Think*, Boston, 2013

- V. MAYER - MUTCHLER- MITCHELL, *Evaluating the privacy properties of telephone metadata*, in *Proceedings of the National Academy of Sciences*, n. 20/2016, 5536 ss., rinvenibile al link *https://pdfs.semanticscholar.org/dbe1/07ce415a8252009f764afa0a058693596c64.pdf?_ga=2.75105106.1789856331.1576169011-2066176090.1576169011*

- V. MAYER SCHONBERGER – T. RAMGE, *Reinventare il capitalismo nell'era dei Big Data*, trad. di G. Maugeri, Egea, 2018

- MCKINSEY GLOBAL INSTITUTE (a cura di), *'Big Data: The Next Frontier for Innovation, Competition, and Productivity'*, 1 (May 2011)

- D. MESSINA, *Il Regolamento (EU) 2016/679 in materia di protezione dei dati personali alla luce della vicenda "Cambridge Analytica"*, in *Federalismi.it*, 24 ottobre 2018

- D. MESSINETTI, voce *Personalità (diritto della)*, in Enc. dir., XXXIII, Giuffrè, Milano, 1983

- D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in Riv. Crit. del Dir. Priv., 1997

- R. MESSINETTI, *Trattamento dei dati per finalità di profilazione e decisioni automatizzate*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Cedam, 2019

- N. MINISCALCO, *DPO obbligatorio per i soggetti pubblici, ma non per tutti: il problema*, rinvenibile al *link https://www.agendadigitale.eu/sicurezza/dpo-obbligatorio-per-i-soggetti-pubblici-ma-non-per-tutti-il-problema/*.

- F. MODAFFERI, *Lezioni di diritto alla protezione dei dati personali, alla riservatezza e all'identità personale*, Lulu.com, Roma, 2015

- J. MONDUCCI – G. SARTOR, *Il codice in materia di protezione dei dati personali. Commentario sistematico al D. Lgs. 30 giugno 2003 n. 196*, Cedam, Padova, 2004

- V. MONGILLO, *L'organismo di Vigilanza nel sistema della responsabilità da reato dell'ente: paradigmi di controllo, tendenze evolutive e implicazioni penalistiche*, in *Responsabilità amministrativa delle società e degli enti (La)*, 2015

- P. MONTALENTI, *Organismo di Vigilanza e sistema dei controlli*, in *Giur. comm*., 2009, I,

- A. MONTI, *Tutela della vita privata, protezione dei dati personali e privacy. Ambiguità semantiche e problemi definitori*, in Diritto di internet, 1/2019

- A. G. MOREZZI, *Modelli Organizzativi ex D. Lgs. n. 231/2001 e assetti adeguati ex art. 2381 c.c.: spunti di riflessione in tema di colpa di organizzazione*, in O. CAGNASSO – M. IRRERA, *Il Nuovo Diritto delle Società*, Numero 14/2008

- F. MUCCIARELLI, *Funzioni e responsabilità dell'organismo di vigilanza*, in A.M. STILE, V. MONGILLO, G. STILE (a cura di), *La responsabilità da reato degli enti collettivi: a dieci anni dal d.lgs. 231/2001. Problemi applicativi e prospettive di riforma*, Napoli, 2013

- D. MULA, *Il trattamento dei dati nel territorio dell'Unione e il meccanismo "one stop shop"*, in S. SICA – V. D'ANTONIO - G. M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, Cedam, Milano, 2016

- A. NISCO*, Responsabilità amministrativa degli enti: riflessioni sui criteri ascrittivi "soggettivi" e sul nuovo assetto delle posizioni di garanzia nelle società*, in *Riv. trim. dir. pen. econ.*, 2004

- C. OGRISEG, *Il Regolamento UE n. 2016/679 e la protezione dei dati nelle dinamiche giuslavoristiche: la tutela riservata al dipendente*, in *Labour & Law Issues*, 2016, n. 2

- E. ONDEI, *Esiste un diritto alla riservatezza?,* in *Rass. dir. Cinema*, 1955

- M. OOSTVEN, *Identifiability and the applicability of data protection to Big Data*, *International Data Privacy Law*, 2016, Vol. 6, No. 4

- U. PAGALLO*, La tutela della privacy negli Stati Uniti d'America e in Europa*, Giuffrè, Milano, 2008

- S. PALANZA, *Internet of things, Big Data e privacy: la triade del futuro*, in *Documenti dell'Istituto Affari Internazionali*, ottobre 2016, rinvenibile al link *www.iai.it*

- P. PALLARO, *Libertà della persona e trattamento dei dati personali nell'Unione Europea,* Giuffré, Milano, 2002

- R. PANETTA, *DPO interno o esterno? Ecco dove si nasconde il conflitto di interessi*, rinvenibile al link
https://www.agendadigitale.eu/sicurezza/privacy/dpo-interno-o-esterno-ecco-dove-si-nasconde-il-conflitto-di-interessi/

- R. PARDOLESI*, Riservatezza: problemi e prospettive*, in M. SPINELLI (a cura di), *Responsabilità civile*, vol. II, Bari, 1974

- R. PARDOLESI, *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*", in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè, Milano, 2003

- R. PARDOLESI, *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè, Milano, 2003

- G. PASCUZZI, *Il diritto dell'era digitale*, Il Mulino, Bologna, 2016

- P. PASSAGLIA – D. POLETTI, *Nodi virtuali legami informali: internet alla ricerca di regole*, *Pisa Univesity Press*, 2017

- E. PELINO, *Identificazione, identificabilità, identificativo*, in BISTOLFI, BOLOGNINI, PELINO, *Il Regolamento Privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè, Milano, 2016

- C. PIERGALLINI, *I Modelli organizzativi*, in LATTANZI (a cura di), *Reati e responsabilità degli enti*, 2a ed., Milano, 2010

- F. PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Le nuove leggi civili commentate*, 2017

- G. PITRUZZELLA, *Big Data, Competition and Privacy: a look from the antitrust perspective*, in *Concorrenza e Mercato*, fasc. 1, 2016

- F. PIZZETTI, *La tutela della riservatezza nella società contemporanea*, Rubbettino, 2010

- F. PIZZETTI, *Gdpr, ecco le vere funzioni del DPO: "attenti, non è un mestiere"*, 25 maggio 2017, rinvenibile al link *https://www.agendadigitale.eu/sicurezza/gdpr-attenti-fare-il-dpo-non-e-un-mestiere-ecco-le-sue-vere-funzioni/*.

- F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, *Dalla dir. 95/46 al nuovo regolamento europeo*, I, Collana *I diritti nella «rete» della rete*, Giappichelli, Torino, 2016

- F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali, Il regolamento europeo 2016/679*, II, Collana *I diritti nella «rete» della rete*, Giappichelli, Torino, 2016

- F. PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018

- D. POLETTI, *Comprendere il Reg. UE 2016/679: un'introduzione*, in P. PASSAGLIA – D. POLETTI, *Nodi virtuali legami informali: internet alla ricerca di regole*, *Pisa Univesity Press*, 2017

- O. POLLICINO, *Un digital right to privavy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain*, in *Dir. Inf.*, 2014

- O. POLLICINO – M. BASSINI, *sub art. 8*, in R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Giuffrè, Milano, 2017

- A. PREDIERI, *L'erompere delle Autorità amministrative indipendenti*, Passigli, Firenze, 1997

- G. RAMACCIONI, *La protezione dei dati personali e il danno non patrimoniale. Studio sulla tutela della persona nella prospettiva risarcitoria*, Jovene editore, Napoli, 2017

- G. RESTA, *Il diritto alla protezione dei dati personali*, in F. CARDARELLI, S. SICA e V. ZENO-ZENCOVICH, *Il codice dei dati personali. Temi e problemi*, Giuffrè, Milano, 2004

- G. RESTA – V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, 2015

- G. RESTA – V. ZENO ZENCOVICH, *La protezione transnazionale dei dati personali, Dai "safe harbour principles" al "Privacy Shield"*, *Roma TrE-Press*, 2016

- A. RICCI, *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, in *Contratto e impresa*, 2017

- G. M. RICCIO, *Data Protection Officer e altre figure*, in S. SICA – V. D'ANTONIO – G. M. RICCIO, *La nuova disciplina europea della privacy*, Cedam, 2016

- G.M. RICCIO - G. SCORZA – E. BELISARIO, *GDPR e Normativa Privacy Commentario*, Wolters Kluver, Milano, 2018

- A ROBNAGEL (a cura di), *Handbuch Datenschutzrech. Die neuen Grundlagen für Wirtschaft und Verwaltung*, Munich, 2003

- S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Laterza, Bologna, 1973

- S. RODOTÀ, *La "privacy" tra individuo e collettività*, in *Politica del diritto*, 1974

- S. RODOTÀ, *Repertorio di fine secolo*, Laterza, Bologna, 1999

- S. RODOTÀ, *I nuovi diritti che hanno cambiato il mondo (Stralcio dell'intervento alle "Lezioni Norberto Bobbio" - Torino 25/10/2004)*, rinvenibile al link *http://www.privacy.it/archivio/rodo20041026.html*

- S. RODOTÀ, *Intervista su Privacy e Libertà*, a cura di Paolo Conti, Editori Laterza, Bologna, 2005

- S. RODOTÀ, *Il diritto di avere diritti*, Editori Laterza, Bari, 2013

- S. RODOTÀ, *Il mondo nella rete. Quali diritti, quali vincoli,* Laterza, Bologna, 2014

- I. S. RUBINSTEIN, *Big Data: The End of Privacy or a New Beginning?* in *International Data Privacy Law*, 2013, Vol. 3, No. 2

- L. RUGGERI – C. PERLINGIERI, *Internet e Diritto Civile*, Edizioni scientifiche italiane, Napoli, 2015

- G. M. RUOTOLO, *I dati non personali: l'emersione dei Big Data nel diritto dell'Unione europea*, in *Studi sull'integrazione europea*, 1/2018

- G. M. SALERNO, *Le origini ed il contesto*, in L. CALIFANO – C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale scientifica, Napoli, 2019

- S. SICA – P. STANZIONE, *Commercio elettronico e categorie civilistiche*, Giuffrè, Milano, 2002

- S. SICA – P. STANZIONE, *La nuova disciplina della privacy. Commento al d.lg. 30 giugno 2003, n. 196*, Zanichelli, Bologna, 2004

- S. SICA, *Verso l'unificazione del diritto europeo alla tutela dei dati personali?*, in S. SICA - V. D'ANTONIO - G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, Cedam, Milano, 2016

- S. SICA – V. D'ANTONIO – G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, Cedam, Milano, 2016

- C. SOLINAS, *La nuova figura del responsabile della protezione dei dati*, in V. CUFFARO – R. D'ORAZIO – V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, 2019

- A. SPINA, *Alla ricerca di un modello di regolazione per l'economia dei dati. Commento al regolamento (Ue) 2016/679*, in *Riv. regolaz. merc.*, 2016

- S. STALLA – A. BOURDILLON - A. KNIGHT, *Anonymous Data v. Personal Data – a False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data*, in *Wisconsin International Law Journal*, 2017

- M.G. STANZIONE, *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Eur. dir. priv.,* 2016

- M. G. STANZIONE, *Genesi ed ambito di applicazione*, in S. SICA – V. D'ANTONIO – G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, Cedam, Milano, 2016

- A. STAZI – F. CORRADO, *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica*, in *Dir. Inf.*, 2019

- M. E. STUCKE – A. P. GRUNES, *Big Data and Competition Policy*, *Oxford University Press*, 2016

- STUDIO LEGALE MONDINI-RUSCONI (a cura di), *Big Data: privacy, gestione, tutele*, *Altalex*, 2018

- R. TORINO, *La valutazione d'impatto (Data Protection Impact Assessment)*, in V. CUFFARO – R. D'ORAZIO – V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019

- E. TOSI (a cura di), *Diritto privato dell'informatica e di Internet*, Giuffrè, Milano, 2006

- E. TOSI, *La responsabilità civile per trattamento illecito dei dati personali*, in E. TOSI (a cura di), *Privacy digitale*, Giuffrè, Milano, 2019

- E. TOSI, *Privacy digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo Codice della Privacy*, in E. TOSI (a cura di) *Privacy digitale*, Giuffrè, Milano, 2019

- C.E. TRAVERSO, *Riservatezza e diritto al rispetto della vita privata*, in Riv. Dir. Industriale, 1963, II

- F. VIOLA, *Data mining. Sottrazione, cessione e utilizzo di dati*, in M. FUMAGALLI MERAVIGLIA (a cura di), *Diritto alla riservatezza e progresso tecnologico*, Editoriale scientifica, Napoli, 2015

- V. ZENO ZENCOVICH, *Profili negoziali degli attributi della personalità*, in *Il diritto dell'informazione e dell'informatica*, 1993

- V. ZENO-ZENCOVICH, P*ersonalità (diritti della)*, in N. LIPARI – P. RESCIGNO (a cura di), *Diritto civile*, Giuffrè, Milano, 2009, I

- V ZENO ZENCOVICH, *Il concetto di "autonomia privata" ai tempi dei "Big Data"*, in P. PASSAGLIA – D. POLETTI, *Nodi virtuali, legami informali: Internet alla ricerca di regole*, Pisa University Press, Atti del Convegno Pisa, 7-8 ottobre 2016

- V. ZENO ZENCOVICH – G. GIANNONE CODIGLIONE, *Ten Legal perspectives on the "Big Data revolution"*, in *Concorrenza e Mercato*, 23

- S. D. WARREN, L. D. BRANDEIS, *The right to privacy*, *Harvard Law Review*, Vol. 4, No. 5 (Dec 15, 1890)

- R. H. WEBER, *Internet of Things – New Security and Privacy Challenges*, in *Computer Law and Security Review*, 2010

- J. Q. WITHMAN, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, in Yale Law Journal, 2004, vol. 113, n. 1

- G. ZICCARDI, *GDPR, multinazionali: requisiti e ruolo del DPO unico*, 24 aprile 2018, reperibile al link *https://www.ipsoa.it/documents/impresa/contratti-dimpresa/quotidiano/2018/04/24/gdpr-multinazionali-requisiti-ruolo-dpo-unico*