La nuova figura del Data Protection Officer nell'UE

Alessia Greco

Sommario

Keywords

Data Protection Officer - GDPR - protezione dei dati personali - privacy - DPO

1. Introduzione

Con l'avvento dell'era digitale e delle sue principali innovazioni, i diritti fondamentali di libertà e dignità umana affrontano sfide non meno gravi di quelle del passato, tanto per l'incontrollata ingerenza di tali tecnologie nella vita di ciascuno di noi, quanto per la diffusa inconsapevolezza e leggerezza con la quale oggi si acconsente a rendere disponibili i propri dati personali in cambio dell'utilizzo di servizi ed applicazioni *smart* apparentemente gratuiti.

L'imprudente cessione del nostro patrimonio informativo, a cui contribuiamo quotidianamente, sottovaluta la successiva trasformazione dei nostri dati personali e le conseguenti compressioni delle nostre libertà: sistemi sempre più raffinati di *data analysis* permettono la raccolta ed il trattamento di una quantità innumerevole di informazioni per diverse finalità, in tempi brevissimi e con costi ridotti, arrivando a ricavare dati importanti dall'incrocio di differenti informazioni in misura potenzialmente infinita.

Ci ritroviamo così in un contesto storico in cui si permette la circolazione e la successiva proliferazione di dati personali capaci di tratteggiare le preferenze, i gusti, le abitudini e le opinioni delle persone, sino a riuscire ad elaborare, con vari gradi di specificità, previsioni sulle future condotte di tutti gli utenti. Ciò poiché un servizio più accurato, e conseguentemente più appetibile per il consumatore, può essere tale solo attraverso il massiccio utilizzo di dati personali, che talvolta non siamo neanche consapevoli di cedere. I vantaggi sono facilmente intuibili e tutti sostanzialmente legati ad una più ottimale ed efficace gestione delle risorse orientate al miglioramento della qualità della vita e del grado di soddisfazione dei consumatori, fornendo loro servizi altamente personalizzati.

Sono altrettanto intuibili, però, le preoccupazioni legate all'acquisizione di sempre più

informazioni personali in violazione della riservatezza dei fruitori e alla potenziale divulgazione a soggetti non autorizzati. Le problematiche sono individuabili anche nella sicurezza collettiva, giacché i più sensibili dati sull'appartenenza ideologica e politica, sesso, razza, etnia, religione, condizione economica e personale, possono essere – e sono stati – abusati da una costante e sistematica manipolazione in chiave repressiva e antidemocratica, così da ingenerare un'esigenza di protezione degli individui contro le intromissioni nella privacy non solo rispetto a privati terzi estranei, ma anche rispetto al potere pubblico.
Risulta pertanto necessario che, con l'avanzare dell'incisività della tecnologia, siano specularmente garantite misure più adeguate, tali da rafforzare diritti già tutelati ma potenzialmente oggetto di sempre maggiori lesioni e limitazioni, difficilmente controllabili nel *World Wide Web*. L'importanza di un dominio sul nostro patrimonio informativo, insieme ad una maggiore cognizione sull'impiego dei nostri dati personali, risultano elementi essenziali al fine di proteggere il nucleo fondamentale delle libertà della persona in un'epoca, come quella odierna, in cui l'utilizzo e lo scambio di informazioni per diverse finalità ha raggiunto il suo picco storico ed è destinato ad aumentare in maniera esponenziale ed irrefrenabile.
Tali considerazioni hanno inevitabilmente imposto al legislatore nazionale ed europeo la necessità di un adeguamento della normativa in materia di *data protection* alle nuove esigenze della società dell'informazione. Il regolamento (UE) 2016/679 è dunque funzionale ad instaurare nell'Unione quel quadro giuridico più solido e coerente in materia di protezione dei dati che possa consentire lo sviluppo dell'economia digitale nel mercato interno, garantendo agli individui il controllo sui loro dati personali per rafforzare la certezza giuridica e al contempo ridurre al minimo gli oneri amministrativi a beneficio delle imprese.

2. La nascita della figura in Germania

Figura chiave nella "nuova" protezione dei dati personali è certamente quella del Data Protection Officer, delineato come un esperto nella tutela dei dati posto sia a baluardo dei diritti degli interessati, sia a supporto dei soggetti attivi del trattamento ai quali fornisce assistenza. Seppur apparentemente confliggenti, i ruoli di difensore e di consulente privacy intendono ampliare la salvaguardia dell'interessato poiché, fornendo consulenza ai soggetti attivi, il DPO svolgerà anche una rigida sorveglianza sul loro operato. È pertanto una figura soggettiva ibrida, che può essere vista come un garante della protezione dei dati interno alla struttura presso cui opera.
L'introduzione di una normativa di applicazione generale è certamente una delle novità principali del regolamento (UE) 2016/679 e ciò testimonia anche il rilievo potenzialmente globale che si è voluto dare al ruolo del DPO sulla scorta dell'efficienza già riscontrata nelle istituzioni ed organismi europei e nelle realtà nazionali che provvidero a disciplinarlo. È infatti il risultato di vari dibattiti, studi ed esperienze maturate nel corso degli ultimi 50 anni laddove, a fronte della generalizzata tendenza a fare uso di archivi informatici e banche dati ed in obbedienza ai principi generali espressi dalla

Convenzione europea dei diritti dell'uomo, a partire dagli anni '70 alcuni Stati europei occidentali cominciarono a riconoscere l'esistenza di un nuovo diritto soggettivo "alla riservatezza" e a dotarsi di discipline nazionali sulla protezione dei dati.
La prima normativa a tutela della privacy fu la *Datenschutzgesetz*, legge regionale tedesca del *Land* di Assia del 1970 che, seppur limitata dalla sola applicazione distrettuale, ha l'importantissimo merito di disciplinare l'istituto del *Datenschutzbeauftragter* (DSB) – Responsabile della protezione dei dati – archetipo dell'attuale Data Protection Officer. Questi veniva designato dal Parlamento regionale, di fronte al quale rispondeva del proprio ufficio, ed aveva il compito di assicurare il rispetto delle norme sulla protezione dei dati personali da parte della pubblica amministrazione e di fungere da punto di riferimento per i cittadini che lamentavano lesioni del proprio diritto alla riservatezza[1].
A livello centralizzato poi, la Germania emanò una prima legge il 27 gennaio 1977, la *Bundesdatenschutzgesetz* (BDSG), in seguito sostituita nel 1990[2] e adeguata alla normativa comunitaria nel 2003. Già cinque anni prima della direttiva 95/46/CE era molto all'avanguardia poiché, oltre a contenere i principi generali poi ripresi dalla normativa comunitaria, prevedeva agli artt. 36 e 37 un'approfondita disciplina sul Responsabile della protezione dei dati, riversatisi poi nei parr. 4f e 4g della nuova legge federale del 2003[3].
Il §4f era dedicato alla nomina del Beauftragter für den Datenschutz (BfD)[4] e sanciva l'obbligo di designazione per: a) enti pubblici che trattavano dati personali con strumenti automatizzati; b) gestori privati che impiegavano almeno nove dipendenti a tempo indeterminato nel trattamento effettuato con sistemi automatizzati; c) tutti i casi di trattamento di dati con mezzi non automatizzati qualora vi fosse un impiego costante di almeno 20 persone.
Il BfD, poi, doveva possedere conoscenze specialistiche in materia di protezione dei dati e, come ovvio, tenere segreta ogni informazione raccolta nell'esercizio delle sue funzioni. Per tale ragione era subordinato direttamente al più alto grado possibile dell'azienda o ente privato in cui operava, così come la sua nomina poteva essere revocata solo su richiesta dell'Autorità di controllo oppure ai sensi dell'art. 626 del Codice civile tedesco (BGB) sul licenziamento per giusta causa. Per garantire ancora di più l'imparzialità della figura, era poi sancito che l'azienda o ente che aveva provveduto alla nomina dovesse anche fornirgli ogni attrezzatura e risorsa necessaria allo svolgimento dei suoi compiti.
Il §4g, invece, esplicava le funzioni del Responsabile della protezione dei dati, stabilendo come fosse tenuto a garantire che le disposizioni della *Bundesdatenschutzgesetz*, e altre normative a tutela della privacy, fossero rispettate, in particolare, monitorando il corretto funzionamento dei programmi informatici per il trattamento dei dati, anche con l'ausilio dell'Autorità di controllo.

---

[1] G. Ziccardi, *Informatica giuridica. Privacy, sicurezza informatica, computer forensic e investigazioni digitali. Tomo II*, Milano, 2012, 13 riportando un pensiero tratto dalla Presentazione di V. Frosini-S. Smitis, *Crisi dell'informazione giuridica ed elaborazione elettronica dei dati*, Milano, 1977, V.

[2] F. Pizzetti-P. Ravaglioli, *Privacy*, in *Diritto privato – Il libro dell'anno 2007*, in *treccani.it*.

[3] Vedi *Bundesdatenschutzgesetz a.F.*, Gazzetta ufficiale federale, Anno 2003, parte I, n. 3, pubblicato il 24 gennaio 2003, in *dejure.org*

[4] K.A. Bamberger-M.K. Deirdre M.K., *Privacy in Europe: Initial Data on Governance Choices and Corporate Practices*, in *The George Washington L. Rev.,* 5(81), 2013, 1574-1576.

In tale normativa, i cui precedenti risalgono già alla legge del 1990, sembra si possano ritrovare numerosi punti di contatto con il successivo regolamento 2001/45/CE[5], primo ad aver istituzionalizzato la figura, e ancor di più con il GDPR e, pertanto, si può certamente ritenere che fu proprio a tale modello che il legislatore europeo si ispirò nel delineamento del Data Protection Officer come lo conosciamo oggi.

3. In Spagna

Anche l'ordinamento spagnolo si premunì di una figura del tutto simile al BfD e all'attuale DPO, prendendo le mosse dalla *Ley orgánica de regulación del tratamiento automatizado de datos de caracter personal*, n. 5/1992 del 29 ottobre[6] – di seguito LORTAD.
Dopo una vigenza di soli 7 anni, stante l'espresso dettato della direttiva 95/46/CE[7], la norma fu abrogata dalla *Ley orgánica de protección de datos* n. 15/1999 del 13 dicembre, cd. LOPD, al fine di ampliare l'ambito di applicazione delle disposizioni estendendole anche al trattamento non o parzialmente automatizzato di dati. Tuttavia, soli sei mesi prima, era appena stato emanato il *Real Decreto* 994/1999[8], contenente il regolamento sulle misure tecniche ed organizzative necessarie a garantire la sicurezza dei sistemi di trattamento soggetti al regime della precedente LORTAD[9]; rimase in vigore anche sotto la vigenza della nuova legge sulla privacy, per poi venir abrogato solo nel 2007 ad opera del *Real Decreto* n. 1720[10] che approvò lo speculare regolamento attuativo della LOPD.
Ebbene, ai fini dell'indagine qui proposta, assume particolare rilevanza il Regolamento del 1999, stante il merito di aver introdotto la figura del *Responsable de seguridad* quale figura «alla quale il responsabile del trattamento ha formalmente assegnato la funzione di coordinare e controllare le misure di sicurezza applicabili»[11], anch'esso antesignano all'attuale Data Protection Officer.
Il *Reglamento de desarrollo* in commento provvide a distinguere tre livelli di misure di sicurezza tecniche ed organizzative, da applicare alle differenti tipologie di dati personali raccolti dall'archivio automatizzato in ragione del diverso grado di tutela necessario. L'art. 4 stabiliva in via generale come tutti gli archivi automatizzati dovessero «adottare

[5] 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 su cui *infra*.

[6] Attraverso tale norma venne soddisfatto il duplice obiettivo del compimento del mandato costituzionale di limitare l'uso dell'informatica per garantire il rispetto dell'onore, dell'intimità personale e familiare ed il pieno esercizio dei propri diritti ai cittadini, di cui all'art. 18 comma 4 Cost. esp., e dell'art. 4 della Convenzione di Strasburgo n. 108/1981; cfr. *Exposición de motivos* nn. 1-3 e art. 1 della *ley* cit.

[7] L. Rebollo Delgado- M. M. Serrano Pérez, *Introducción a la protección de datos*, Madrid, 2008, 55.

[8] Con il quale veniva approvato il *Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.*

[9] Vedi art. 1, *Real Decreto 994/1999, de 11 de junio.*

[10] *Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.*

[11] Ivi, num. 11), art. 2 testualmente dispone: «*Responsable de seguridad: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables*».

le misure di sicurezza qualificate di livello minimo»[12], mentre gli archivi contenenti un insieme di dati che congiuntamente avrebbero consentito una valutazione sulla personalità del soggetto cui si riferivano, avrebbero dovuto «soddisfare, oltre che le misure di livello minimo, quelle qualificate di livello medio»[13]. Infine, nel caso in cui l'archivio avesse trattato i c.d. dati sensibili oppure informazioni raccolte ai fini dell'applicazione della legge, si sarebbe dovuto garantire «oltre che le misure di livello minimo e medio, quelle qualificate di livello alto»[14]. Il regolamento proseguiva elencando dall'art. 8 al 26 le varie misure di sicurezza, distinte per l'intensità di tutela che assicuravano e, tra queste, il *Responsable de seguridad* (RS) quale misura classificata di livello medio ed alto.
Dunque, mentre Germania, Paesi Bassi, Svezia, Lussemburgo e Francia adottavano il sistema alternativo di notificazione suggerito dall'art. 18, par. 2, della direttiva 95/46/CE nominando un «incaricato della protezione dei dati», peculiare la Spagna, nella quale vigeva l'obbligo di nomina del RS quale misura tecnico-organizzativa di sicurezza per quei trattamenti ritenuti bisognosi di un livello medio o alto di tutela.
Era il soggetto incaricato del coordinamento e del monitoraggio delle misure di sicurezza messe in atto dal responsabile dell'archivio nel documento di sicurezza[15] e, nonostante fosse lo stesso responsabile a nominarlo, l'art. 16 sanciva come tale circostanza non avrebbe comunque supposto un'esenzione di responsabilità per il designante nell'attuazione della legge sulla tutela dei dati. Altra funzione del Responsabile della Sicurezza veniva fissata dal par. 3 del seguente art. 17: era incaricato di analizzare le relazioni di verifica sullo stato di sicurezza[16], così da fornire al responsabile dell'archivio indicazioni circa le migliorie da apportare alle misure di sicurezza già predisposte[17]. Inoltre, solo quando nominato per integrare una misura di sicurezza di livello alto, era incaricato anche di esaminare regolarmente le informazioni fornite dal registro degli accessi, ulteriore e distinta misura di livello alto[18].
Il successivo *Real Decreto* n. 1720/2007 abrogò esplicitamente il Regolamento del 1999 e, pur predisponendo una disciplina molto più amplia in ossequio alla mutata normativa comunitaria, non modificò le disposizioni in commento, lasciando la figura del Responsabile della Sicurezza sostanzialmente intatta. Unica eccezione riguardava la previsione del nuovo art. 109, il quale ampliava l'ambito di applicazione delle norme

[12] Ivi, art. 4, par. 1.

[13] Ivi, art. 4, par. 2, e par. 4.

[14] Ivi, art. 4, par. 3.

[15] Il *documento de seguridad* è il documento mediante il quale il responsabile dell'archivio elabora ed adotta le misure tecniche ed organizzative necessarie per garantire la sicurezza di livello minimo dei dati di carattere personale, la sua adozione è infatti obbligatoria per qualsiasi trattamento di dati personali. È disciplinato dagli artt. 8 e 15, ivi, che fissano il differente contenuto rispetto al diverso livello di sicurezza richiesto.

[16] Gli *informes de auditoría* sono disciplinati dall'art. 17, ivi, quali strumenti di valutazione interni o esterni sui sistemi di informazione ed elaborazione dati, catalogati come misure di sicurezza di livello medio.

[17] Ivi, art. 17, par. 2.

[18] Per gli archivi catalogati come bisognosi di un alto livello di protezione era da conservare, per un massimo di 2 anni, il registro degli accessi, che deve contenere almeno l'identificativo dell'utente, data ed ora di accesso, l'archivio consultato e l'autorizzazione o denegazione all'accesso. Così il par. 1 dell'art. 24, ivi: «*De cada acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado*».

sul *Responsable de seguridad* in relazione agli archivi non automatizzati, precedentemente esclusi dall'ambito di applicazione dalla LORTAD.
Come si vedrà più avanti rispetto alla direttiva 95/46/CE e al regolamento 45/2001, può già osservarsi come anche l'ordinamento spagnolo abbia influenzato, seppur in maniera meno pervasiva rispetto alla disciplina tedesca, il delineamento della figura del *Personal data protection official* prima e del Data Protection Officer poi. Si noti difatti come, a differenza della *Bundesdatenschutzgesetz*, entrambi i regolamenti comunitari prevedono l'obbligatorietà della nomina[19] non in relazione alle dimensioni del titolare del trattamento, ma rispetto alla tipologia di dati trattati similmente al *Reglamento de desarrollo* 15/1999.

4. Il Data Protection Officer nelle fonti comunitarie

A livello sovranazionale poi, un primo riferimento al DPO lo ritroviamo al par. 2 dell'art. 18 della direttiva 95/46/CE che, sebbene non lo abbia puntualmente disciplinato, già prevedeva la possibilità di nomina di un soggetto simile.
L'"incaricato della protezione dei dati"[20] era previsto solo quale misura alternativa all'obbligo di notifica dei trattamenti interamente o parzialmente automatizzati all'Autorità di controllo in capo al «responsabile del trattamento»[21] di cui al par. 1. Il menzionato par. 2 consentiva agli Stati membri, attraverso le norme di attuazione della direttiva, di stabilire una semplificazione della procedura di notifica, sino al totale esonero dall'obbligo per il titolare del trattamento che avesse designato un *personal data protection official*; erano a lui demandati i compiti di tenuta del registro dei trattamenti, effettuati dal designante, e di salvaguardia sull'applicazione interna delle disposizioni della direttiva, al fine di garantire che il trattamento non fosse «tale da recare pregiudizio ai diritti e alle libertà della persona interessata».
Furono solo Germania, Paesi Bassi, Svezia, Lussemburgo e Francia ad adottare tale sistema di notificazione alternativo[22], i cui risultati rappresentarono la base su cui la figura fu più rigorosamente disciplinata ed imposta alle istituzioni e agli organismi comunitari dal successivo regolamento 45/2001 e, in seguito, dal regolamento (UE) 2016/679.
Nonostante le esperienze positive di tali ordinamenti, le Istituzioni europee registravano una certa indifferenza a tale figura da parte di molti Stati membri infatti, sia la Com-

[19] La cui infrazione è considerata grave, in una scala di sanzioni che ricomprende infrazioni lievi, gravi a gravissime.

[20] Nella versione originale denominato "*personal data protection official*".

[21] La figura comunitaria del «responsabile del trattamento» viene recepita nell'ordinamento italiano con la denominazione di "titolare del trattamento", la disposizione è dunque da riferire a tale figura soggettiva.

[22] Article 29 Working Party, *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*, WP106, Bruxelles, 18 gennaio 2005, in *gpdp.it*.

missione europea[23], sia l'Article 29 Working Party[24] auspicavano ad un più massiccio utilizzo del *privacy officer* affinché contribuisse ad un concreto risparmio sulle onerose attività di notifica dei trattamenti al Garante e ad un'applicazione più uniforme della direttiva.

In tale ottica si ebbe un importante passo in avanti con l'emanazione del regolamento comunitario 45/2001 già menzionato, i cui artt. 24 e seguenti hanno compiutamente delineato la figura del DPO in combinato disposto con l'Allegato Unico, rendendone obbligatoria la nomina per le istituzioni e gli organismi comunitari.

Il Regolamento disponeva un obbligo di nomina del Responsabile della protezione dei dati in capo ad «ogni istituzione ed organismo della Comunità» e gli affidava la funzione di rendere edotti tanto i responsabili quanto gli interessati sui diritti e gli obblighi ivi previsti, di cooperare con il Garante europeo della protezione dei dati – istituito in tale sede, di garantire un'applicazione imparziale delle norme, di tenere il registro dei trattamenti e di notificare al Garante europeo i trattamenti considerati ad alto rischio per i diritti delle persone fisiche.

L'art. 24 proseguiva indicando come il Data Protection Officer dovesse essere scelto «in funzione delle sue qualità personali e professionali e, in particolare, delle sue conoscenze specifiche in materia di protezione dei dati»; la nomina, di durata da 2 a 5 anni e rinnovabile per una sola volta, non poteva dar luogo a conflitti d'interesse rispetto ad eventuali ulteriori incarichi in quanto in ogni caso preminente. Tale previsione, in aggiunta al divieto imposto alle istituzioni di impartirgli istruzioni e all'obbligo di fornirgli tutto il personale e le risorse necessari, ne garantiva l'indipendenza da qualsiasi pressione interna. L'art. 25, invece, prevedeva l'obbligo in capo ai designanti di notificare al DPO qualsiasi operazione avessero intenzione di eseguire sui dati personali senza indugio, i quali venivano conservati dal Responsabile della protezione nel registro dei trattamenti, regolamentato dal successivo art. 26.

Peculiare è la predisposizione di un unico Allegato al Regolamento, contenente sì poche disposizioni, ma tutte volte a specificare i compiti e le facoltà del Responsabile della protezione, lasciando trasparire una chiara propensione per la nomina di un DPO esterno all'organizzazione designante o che comunque non rivestisse ulteriori e differenti compiti. Il legislatore ha infatti ritenuto che, per non gravarlo di un onere eccessivo, fosse da preferire un soggetto che potesse ricoprire il solo ruolo di DPO poiché, designando un dipendente già impiegato in altra posizione, facilmente avrebbe potuto trovarsi in conflitto con le sue funzioni ordinarie, specialmente se sollevato solo parzialmente da esse. Ugualmente problematico, nell'eventualità di nomina di un soggetto interno, sarebbe risultata la tematica del necessario grado d'indipendenza di cui il DPO doveva godere: l'istituzione o organismo designante sarebbe in tal caso risultato contemporaneamente tanto superiore gerarchico, quanto titolare del trattamento da sorvegliare, causando un'eccessiva influenza sullo svolgimento dei compiti del Data

[23] Relazione della Commissione, *First report on the implementation of the Data Protection Directive (95/46/EC)* – COM(2003) 265 def., Bruxelles, 15 maggio 2003, 27.

[24] Article 29 Working Party, *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*, cit.

Protection Officer[25].
Estremamente rilevante risulta il ruolo consultivo qui assegnato al DPO, successivamente ancor più sviluppato dal regolamento (UE) 2016/679: era ritenuta principale l'attività di supporto ai soggetti del trattamento in quanto figura in grado di interpretare la normativa, così da renderla di immediata comprensione a tutti i soggetti operanti nell'azienda ed orientarne l'azione anche rispetto ai cambiamenti legislativi.
Nonostante la rilevanza del regolamento 45/2001, tuttavia, il limitato ambito di applicazione dal quale esulano i soggetti pubblici e privati degli Stati membri non ha consentito la diffusione desiderata e, vista anche la scarsa regolamentazione della direttiva 95/46/CE in materia, si è dovuto attendere il GDPR per giungere ad una razionalizzazione completa del sistema e all'istituzionalizzazione del professionista privacy come auspicato dalle autorità europee.

5. Il DPO nel General Data Protection Regulation

Alla luce di quanto detto, appare chiaro come la semplificazione delle operazioni di notifica all'Autorità di controllo nazionale sia stata un'esigenza di cui il legislatore europeo non ha potuto non tenere conto e, conseguentemente, quanta importanza rivesta in tal senso una disciplina dettagliata del Data Protection Officer.
Il regolamento (UE) 2016/679 lo delinea come un garante della protezione dei dati interno alla struttura presso cui opera, infatti consente sia all'Autorità di controllo che all'interessato di trovare in lui un "punto di contatto" per rendere la tutela dei dati maggiormente capillare, eliminando *in nuce* la necessità che giustificava l'obbligo di notifica al Garante nazionale. Si colloca in una posizione intermedia tra il titolare e/o il responsabile del trattamento e l'Autorità di controllo poiché è tenuto, non solo ad informare e consigliare il responsabile, ma anche a monitorare internamente l'applicazione della normativa a protezione dei dati personali e, oltre a giovare i soggetti attivi con un risparmio economico nel lungo periodo, consente di apprestare la tutela più ampia possibile ai dati personali trattati, valutandone i rischi sin dal principio del trattamento; è infatti qualificato come un "professionista della privacy".
Spingendo enti ed aziende a nominare un DPO – perché obbligate dal GDPR o invogliate a dimostrare la propria *accountability*, il Regolamento ha finalmente ottemperato alle richieste delle autorità europee di razionalizzare le procedure di notifica, riuscendo «concretamente a diminuire gli oneri amministrativi e ridurre i costi dei responsabili del trattamento»[26]. Ai sensi del considerando 86 infatti, scompare l'obbligo per il titolare di notificare i trattamenti al Garante sancito dalla direttiva 95/46/CE, sostituito da quello di nominare un DPO nei casi di cui al par. 1 dell'art. 37. L'obbligo di notifica del titolare al Garante, infatti, è ora predisposto per le sole ipotesi di *data breach* e di

[25] Così il Garante Europeo della Protezione dei Dati nel *Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001*, Bruxelles, 28 novembre 2005, 4-5, in edps.europa.eu.

[26] Così Comunicazione della Commissione al Parlamento Europeo al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *A comprehensive approach on personal data protection in the European Union*, COM(2010) 609 def., Bruxelles, 4 novembre 2010, 11.

consultazione preventiva in caso di valutazione negativa del DPIA[27].
Il Regolamento dedica al DPO l'intera Sezione 4 del Capo IV, i cui artt. 37, 38 e 39 si occupano rispettivamente della sua designazione, della posizione rispetto agli altri soggetti del trattamento e dei compiti di cui è incaricato.
La designazione è onere sia dal titolare che dal responsabile, a seconda del soggetto che soddisfi i criteri relativi alla nomina[28] ed è resa obbligatoria dall'art. 37 per ogni autorità ed organismo pubblico – ad esclusione delle autorità giurisdizionali – e per ogni impresa privata le cui attività principali consistano in «trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedano il monitoraggio regolare e sistematico degli interessati su larga scala» o riguardino trattamenti «su larga scala» di dati cdd. sensibili o giudiziari. Si rinviene qui un certo richiamo all'ambito di applicazione del BfD tedesco, anche se il limite numerico ivi sancito per la designazione è stato sostituito con una più opportuna valutazione sulla tipologia di trattamenti effettuati, in maniera del tutto simile al RS spagnolo. La Proposta di Regolamento conteneva, infatti, una previsione secondo cui l'obbligo di nomina sarebbe stato da imporre alle aziende con più di 250 dipendenti, ma l'Article 29 Working Party rilevò come quello della dimensione della struttura non fosse un criterio adatto a stabilire l'effettiva necessità di un professionista della privacy, in quanto organizzazioni con meno di 250 dipendenti che trattassero ingenti quantità di dati o compissero trattamenti altamente rischiosi, avrebbero potuto necessitare di un DPO ancor più delle grandi aziende le cui attività di trattamento fossero del tutto marginali[29]. Il WP29 suggerì dunque che, rispetto alla quantità di dipendenti dell'azienda, sarebbe stato più utile utilizzare, come già in Spagna, un criterio basato sulla natura o la mole dei trattamenti effettuati, oppure sul numero soggetti direttamente impiegati al trattamento dei dati personali come in Germania, e non sulla generale quantità di impiegati.
Circa la nozione di autorità pubblica ed organismo pubblico cui si riferisce la lett. a) dell'art. 37, sono da ritenere tali le persone giuridiche così inquadrate dal diritto interno[30]; non vengono specificate le dimensioni dell'organismo destinatario dell'obbligo e può essere designato anche un unico Data Protection Officer per più autorità o organismi pubblici «tenuto conto della loro struttura organizzativa e dimensione» per disposizione del par. 3, previsione potenzialmente molto utile per ridurne i costi e garantire la pronta reperibilità del *privacy officer* negli enti di piccole dimensioni.
Al di fuori di tali casi, invece, l'indagine sui soggetti privati tenuti alla nomina riporta a differenti concetti. Innanzitutto, sono da prendere in considerazione le tipologie di attività intraprese dal titolare, laddove saranno "principali", ai sensi del considerando 97, le sole attività primarie e non anche quelle accessorie di trattamento dei dati per-

[27] Titolare e/o responsabile saranno obbligati a richiedere una consultazione preventiva al Garante sui risultati del DPIA nelle sole ipotesi di trattamento espressamente indicati dalla legislazione di armonizzazione o qualora la valutazione «indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio», cfr. art. 36 GDPR.

[28] S. Comellini, *Il responsabile della protezione dei dati: Data Protection Officer DPO aggiornato al d. lgs. del 10 agosto 2018, n. 101 in materia di privacy*, Santarcangelo di Romagna, 2018, 30.

[29] Article 29 Working Party, *Opinion 01/2012 on the data protection reform proposals*, WP191, 29 marzo 2012, 16.

[30] Article 29 Working Party, *Guidelines on Data Protection Officers*, WP243, 13 dicembre 2016, 8.

sonali, sempreché queste non siano attività necessarie alla finalità ultima perseguita dal titolare[31].

Queste, poi, devono configurarsi o quali trattamenti di dati comuni consistenti nel «monitoraggio regolare e sistematico degli interessati», oppure come trattamenti di dati cdd. sensibili o giudiziari, sempreché entrambi effettuati «su larga scala». Il Regolamento non definisce tali concetti, però il WP29[32] indica che, se indubbiamente il monitoraggio ricomprende la profilazione e il tracciamento online, come desumibile anche dal considerando 24, ne esistono ulteriori forme meno palesi ma ugualmente pericolose[33].

Circa il concetto di «larga scala» poi, il considerando 91 indica le attività «che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato». Il WP29 ugualmente fatica a tracciarne contorni definiti, ma menziona la quantità di interessati, il volume e/o le diverse tipologie di dati trattati, la durata delle attività e l'ampiezza geografica dell'attività di trattamento quali utili parametri in base ai quali determinare l'ampiezza dei trattamenti[34].

Dunque, i titolari che effettuino trattamenti di tale portata sui dati sensibili dell'art. 9 o i dati giudiziari dell'art. 10, oppure attraverso meccanismi qualificabili come monitoraggio regolare e sistematico, saranno colpiti dall'obbligo *ex* art. 37, par. 1 di nominare un Data Protection Officer mentre, al di fuori di tali circostanze, la nomina resta una facoltà riconosciuta ai soggetti attivi del trattamento[35] che, se esercitata, ne dimostra in concreto l'*accountability*.

In relazione alla durata dell'incarico, poi, la norma non stabilisce un termine massimo, a differenza del regolamento 2001/45/CE, tuttavia recentemente il Consiglio dell'Autorità Nazionale Anticorruzione, in merito alle nomine in organismi pubblici, si è espressa in merito alla necessità di ottemperare ai principi fissati dall'art. 36 del Codice dei contratti pubblici, in particolar modo a quello di rotazione[36]: la Pubblica Amministrazione, sin dalla predisposizione del bando di gara per il conferimento dell'appalto di servizio, ha l'onere di fissare una durata dell'incarico del DPO esterno che sia congrua rispetto gli obbiettivi perseguiti e, se dal caso, l'opzione di rinnovo del contratto per una durata predeterminata. Per non frustrare il principio di rotazione, dunque, il reinvito o l'affidamento al soggetto uscente deve rivestire carattere eccezionale, sostenuto da motivazioni stringenti, ad esempio «attinenti alla particolare strut-

[31] G.M. Riccio, *sub.* artt. 37-38, in G.M. Riccio-G. Scorza-E. Belisario (a cura di), *GDPR e normativa privacy. Commentario,* Milano, 2018, 342.

[32] Ivi, 343.

[33] Le *Guidelines on Data Protection Officers* del WP29, cit., chiariscono che le ipotesi che integrano una regolarità e sistematicità, sancendo che è regolare quel monitoraggio «che avviene in modo continuo 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», mentre sistematico è quello «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», 11.

[34] Ivi, 10.

[35] Cfr. art. 37, par. 4, GDPR.

[36] ANAC, delibera n. 421 del 13 maggio 2020: *"Richiesta di parere in merito all'applicazione del principio di rotazione ai contratti aventi ad oggetto il servizio di protezione dei dati personali (DPO)"* in *anticorruzione.it*

tura del mercato e alla riscontrata effettiva assenza di alternative, che non sembrano ricorrere nel caso di specie».

In ordine alla provenienza del DPO, invece, il par. 6 dell'art. 37 consente la scelta tanto di un soggetto interno alla struttura del designante, quanto di una persona fisica o giuridica esterna nominata attraverso un contratto di servizi che sia, secondo quanto affermato da ultimo dalla giurisprudenza amministrativa[37], dipendente della società cui è affidato l'incarico. Anche in relazione al ruolo del DPO in commento restano valide le considerazioni proposte in relazione al regolamento 45/2001 circa l'opportunità di nomina di un *privacy officer* esterno, stante la medesima possibilità di conflitti d'interesse che potrebbero venir in essere e, soprattutto, di limitazione delle funzioni di DPO rispetto alle mansioni ordinarie[38]. Per ovviare a tale problematica è stato anche suggerito di determinare *ex ante* una differenziazione della quantità di tempo da dedicare alle une e alle altre funzioni, tenendo anche in conto la possibilità che il DPO possa dover abbandonare improvvisamente i suoi compiti ordinari in caso di circostanze urgenti, vedasi la *data beach*[39].

Prescindendo dalla radice del soggetto, è richiesto il possesso di specifici requisiti: è un tecnico professionista della protezione dei dati personali che, ai sensi del par. 5, dev'essere selezionato «in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti» assegnatigli dalla normativa sulla *data protection* e dall'eventuale contratto di servizi. Il riferimento alla conoscenza "specialistica" pare ricollegarsi alla figura del giurista, quale professionalità capace di interpretare sistematicamente le norme cui conformarsi – funzione del DPO fissata dalla lett. a), par. 1, art. 39. Non esistono ad oggi, tuttavia, albi professionali attraverso cui documentare detta conoscenza[40], ma può rivelarsi indicativa in tal senso il possesso della Certificazione UNI 11697:2017 su cui *infra*.

Sono il titolare e/o il responsabile del trattamento che, designando il DPO, dovranno valutare se questi soddisfi tali requisiti richiesti, facendo riferimento anche alla tipologia di trattamenti, alla quantità di dati trattati ed al livello di protezione auspicato. Dei requisiti riscontrati dovrà essere dato conto al Garante[41] attraverso la redazione di una motivazione da fornire all'atto della nomina, così da valutare la conformità della nomina e l'indice di *accountability* dei soggetti attivi, dimostrando in tal modo la capacità di scegliere un soggetto realmente competente in relazione ai rischi cui sono esposti i dati che trattano.

L'art. 38 si occupa della posizione del DPO, stabilendo innanzitutto un obbligo di informazione a carico sia del titolare che del responsabile del trattamento i quali devono far sì che «sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali» e fornirgli tutte le risorse necessarie all'a-

[37] TAR Puglia, sez. III, 13 settembre 2019, n. 1468.

[38] Così il Garante Europeo della Protezione dei Dati nel *Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001*, cit.

[39] G.M. Riccio, s*ub.* artt. 37-38, *GDPR e normativa privacy. Commentario*, cit., 346.

[40] Ivi, 345.

[41] *Ibid.*

dempimento dei suoi compiti, compresa la formazione continua di cui abbia bisogno. Tali previsioni hanno un importante risvolto nell'ottica dell'autonomia della figura poiché, pur essendo da loro nominato, questi non è a loro subordinato, ma il *privacy officer* riferisce direttamente ai loro superiori gerarchici e può essere destituito dal ruolo solo ed esclusivamente qualora non soddisfi più le condizioni richieste per l'esercizio delle sue funzioni. In ragione di ciò, il Garante consiglia la nomina di un dirigente o di un funzionario di alta professionalità nei casi di DPO interno, cosicché possa svolgere le proprie funzioni in autonomia ed in stretta collaborazione con i soggetti apicali della struttura[42]. A prescindere poi dalla posizione interna o esterna del professionista, titolare e responsabile devono di assicurarsi che, vista la primaria importanza dei compiti di DPO, ogni altra mansione affidatagli sia con questi compatibile al fine di evitare qualsiasi conflitto d'interesse.

Le funzioni del Data Protection Officer sono enumerate dall'art. 39 del GDPR e possono riassumersi nell'attività di vigilanza sulla conformità delle operazioni di trattamento, nella consulenza fornita a titolare, responsabile e relativi dipendenti sul rispetto delle norme in materia di *data protection* – compresi i pareri delle Autorità comunitarie e nazionali di controllo[43] – e nel ruolo di cooperazione e contatto tra i soggetti attivi del trattamento, l'interessato e l'Autorità di controllo. La circostanza per cui il DPO sia incaricato "almeno" dei compiti fissati dall'art. 39, chiarisce la natura aperta e non tassativa dell'elenco, stante la possibilità di ampliamento e specificazione delle funzioni attraverso l'eventuale contratto di servizi con cui può essere nominato. Tra i compiti liberamente determinabili certamente rientra la tenuta del registro delle attività di trattamento, attribuzione ormai tipica nella prassi invalsa[44].

Interessante come la funzione di sorveglianza sulla corretta osservanza della normativa e degli obblighi di *compliance* sia stata nettamente dilatata: nella direttiva 95/46/CE veniva indicata in maniera generica ed era comunque scissa dal principio di responsabilizzazione, faro del regolamento (UE) 2016/679, mentre nel regolamento del 2001 tale funzione era alquanto marginale rispetto al prevalente ruolo consultivo ed informativo. Inoltre, il ruolo di sensibilizzazione sulla normativa privacy è stato affiancato e messo in ombra dalla preminente funzione di cooperazione che, seppur già prevista dal regolamento 2001/45/CE, viene ampliata dal proattivo GDPR, il quale configura il DPO un "punto di contatto", referente tanto dei soggetti designanti quanto di interessati ed Autorità di controllo.

Le norme evidenziate trovano evidentemente un importante precedente nelle discipline suesposte, in particolare nella *Bundesdatenschutzgesetz* e nel Regolamento 2001/45/CE. Ci si riferisce all'obbligatorietà della nomina, ai requisiti professionali del DPO – del tutto assenti nella direttiva 95/46/CE, alla garanzia sull'indipendenza della figura, alla funzione di sorveglianza sul corretto adempimento della normativa e, per ciò che attiene al solo Regolamento, al germe del ruolo consultivo. Lo spagnolo *Real decreto* 994/1999, invece, non precisava le competenze che avrebbe dovuto possedere

[42] Ivi, 346.

[43] G.M. Riccio, s*ub.* art. 39, *GDPR e normativa privacy. Commentario,* cit., 350.

[44] S. Comellini, *Il responsabile della protezione dei dati: Data Protection Officer DPO aggiornato al d. lgs. del 10 agosto 2018, n. 101 in materia di privacy*, cit., 54.

il professionista, né il criterio dell'indipendenza, tuttavia anche in tale contesto era disposto che il Responsabile della Sicurezza doveva essere designato in virtù di un criterio basato sulla natura dei trattamenti effettuati e che la sua nomina non supponeva un'esenzione di responsabilità nell'attuazione delle norme per il designante, così come veniva puntualmente descritta la funzione di sorveglianza sulla corretta applicazione della normativa.

6. Il recepimento della disciplina in Italia attraverso il d. lgs. 101/2018

Nonostante la natura di atto *self-executing* del regolamento (UE) 2016/679, è stato lasciato agli Stati membri un certo margine discrezionale per adottare norme di settore specifiche, purché conformi allo stesso. In Italia il quadro normativo è stato completato attraverso il decreto legislativo di armonizzazione n. 101 del 2018[45], necessario da un lato ad abrogare espressamente quelle disposizioni del "Codice privacy" del 2003 non più compatibili, e dall'altro ad integrare e modificare le disposizioni ancora applicabili per adeguare l'ordinamento al nuovo approccio basato sul rischio e al principio dell'*accountability*.

Per ciò che attiene alla figura del DPO, questa era del tutto sconosciuta all'ambito normativo italiano, il quale non era stato così lungimirante da avvalersi della possibilità di derogare all'obbligo di notifica dei trattamenti al Garante previsto dall'art. 18 della direttiva 95/46/CE ma, nonostante ciò, può rilevarsi un certo richiamo al *privacy officer* da parte di alcune figure già note all'ordinamento per le medesime finalità di prevenzione del rischio[46].

Nel recepimento delle disposizioni sul Data Protection Officer, il decreto di armonizzazione ha ovviato all'assenza di regolamentazione addirittura ampliando l'ambito di applicazione del Responsabile della Protezione dei Dati, facendo così tesoro dell'indicazione del par. 4 dell'art. 37 del GDPR che dava al diritto nazionale la possibilità di prevedere ulteriori ipotesi di designazione obbligatoria. Infatti l'art. 2-*sexiesdecies* del Codice privacy, inserito dal d.lgs. 101/2018, ha esteso l'obbligatorietà della nomina del RPD anche «ai trattamenti di dati personali effettuati dalle autorità giudiziarie nell'esercizio delle loro funzioni», ipotesi espressamente esclusa dal novero delle circostanze obbligatorie dell'art. 37 par.1 del Regolamento.

Non si rilevano ulteriori disposizioni innovative relative alla figura del DPO, proba-

[45] Decreto Legislativo 10 agosto 2018, n. 101, "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" adottato in virtù della delega all'Esecutivo contenuta dall'art. 13 della legge n. 163/2017 per l'adeguamento della normativa nazionale alle disposizioni del GDPR, conosciuta anche come "Legge di delegazione europea 2016-2017".

[46] Aa. Vv., *Il processo di adeguamento al GDPR. Aggiornato al D.lgs. 10 agosto 2018, n. 101*, Milano, 2018, 176, in riferimento al Responsabile per la prevenzione della corruzione e della trasparenza (RPC), disciplinato dalla l. 190/2012, e all'Organismo di vigilanza previsto dal d.lgs. 231/2001 sulla responsabilità degli enti da reato.

bilmente anche a causa dello scarno lavoro di specificazione effettuato dal legislatore italiano, ma molto importante, di contro, l'attività del Garante italiano, che ha precisato alcuni aspetti della normativa europea poco chiari. Innanzitutto, indica «come scegliere il responsabile della protezione dati» attraverso la newsletter n. 432 del settembre 2017[47], specificando che il DPO dev'essere scelto sulla base di competenze ed esperienze specifiche che dimostrino un'approfondita conoscenza delle norme e delle prassi in materia di protezione dei dati personali e la padronanza delle norme che disciplinano il particolare ambito di riferimento nel quale si inserisce la nomina. Il Garante prosegue specificando come l'attestazione delle qualità professionali richieste non pretenda né il possesso di particolari certificazioni, né tantomeno l'iscrizione ad appositi albi professionali, non (ancora) previsti dalla normativa attuale.
A tal riguardo, l'Ente Nazionale Italiano di Unificazione ha predisposto la norma tecnica UNI 11697:2017 "Attività professionali non regolamentate - Profili professionali relativi al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza", in vigore dal 30 novembre 2017. Questa individua e definisce le conoscenze, abilità e competenze dei profili professionali relativi al trattamento e alla protezione dei dati personali, in particolare per le Tecnologie dell'Informazione e della Comunicazione (ICT); è stata elaborata in coerenza con il Quadro Europeo delle Qualifiche (European Qualification Framework – EQF) e utilizzando gli strumenti messi a disposizione dalla UNI 11621-1 sulle "Attività professionali non regolamentate - Profili professionali per l'ICT - Parte 1: Metodologia per la costruzione di profili professionali basati sul sistema e-CF"[48]. Un approccio simile è stato quella della Spagna, laddove è stato adottato lo Schema di certificazione non obbligatorio dell'Agencia Española de Protección de Datos, tuttavia si dubita sulla loro effettiva utilità visto il mancato riconoscimento tanto a livello europeo quanto regionale.
Sul punto si consideri come il Regolamento UE guardi con generale favore all'adozione di codici di condotta di categoria e a certificazioni quali meccanismi di *accountability* atti a dimostrare l'ottemperanza agli obblighi e ai principi del GDPR, ragion per cui anche la designazione di un DPO che possegga adeguate competenze professionali certificate da un soggetto terzo imparziale può rappresentare un ulteriore elemento di responsabilizzazione[49]. Nonostante ciò, tuttavia, la normativa attuale non prevede l'obbligo per i candidati di essere forniti di attestazioni formali; sono certamente da privilegiare soggetti che possano dimostrare di possedere tali competenze attraverso documentazioni fornite da soggetti terzi, quali attestati di partecipazioni a Master e a corsi di studio o professionali, tuttavia il Garante precisa che certificazioni simili, pur costituendo titolo preferenziale, non attribuiscono di per sé una qualifica o un'abilitazione professionale all'aspirante DPO e, pertanto, non possono sostituirsi al necessario processo di selezione[50].

---

[47] Garante per la Protezione dei Dati Personali, *Regolamento privacy, come scegliere il responsabile della protezione dei dati. Le prime indicazioni del Garante: necessarie competenze specifiche non attestati formali*, 15 settembre 2017, doc. web 6826945.

[48] Vedi scheda informativa *ICT: protezione dei dati personali*, in *uni.com*.

[49] S. Napoli, *La figura del Data Protection Officer nel nuovo Regolamento Europeo*, in *AIEA*, maggio 2017.

[50] Nonostante ciò, dall'a.a. 2018/2019 è attivo presso il Politecnico di Milano il Master universitario

Indicativa in tal senso la sentenza n. 287/2018 del TAR del Friuli-Venezia Giulia con la quale il giudice amministrativo ha annullato la procedura concorsuale in cui un'azienda sanitaria pubblica richiedeva, tra i requisiti di ammissione al bando di concorso, anche il possesso della certificazione di "*Auditor* o *Lead Auditor* per i Sistemi di Gestione per la Sicurezza delle Informazioni"[51]. Il Tribunale ritenne che quest'ultima non potesse costituire titolo abilitante allo svolgimento dei compiti di DPO, quale standard di «prevalente applicazione nell'ambito dell'attività d'impresa», il quale certifica la capacità di predisporre meccanismi atti ad incrementare l'efficienza e la sicurezza nella gestione delle informazioni che «non coglie la specifica funzione di garanzia insita nell'incarico conferito». Ciò poiché il DPO è votato alla tutela del diritto fondamentale alla protezione dei dati, a prescindere dagli strumenti utilizzati e, pertanto, la certificazione avrebbe potuto certamente rappresentare un titolo curriculare, ma non anche un «titolo formativo o abilitante, come tale idoneo ad assurge a requisito di accesso»; a fronte di tali motivi il TAR provvide ad annullare la procedura di selezione.

7. L'adeguamento del legislatore spagnolo: la nuova LOPD

Il GDPR si inserì nell'ordinamento spagnolo attraverso l'adozione del *Real Decreto-ley* n. 5/2018[52], volto a predisporre le necessarie misure urgenti di adattamento alla nuova normativa, e con la successiva legge organica[53] sulla protezione dei dati finalizzata a consentire la piena armonizzazione della disciplina agli standard fissati dal Regolamento europeo.

Per ciò che attiene in particolare alla figura del Responsabile della protezione dei dati, questi assumeva la denominazione di *Delegado de protección de datos* – DPD nella *Ley Orgánica* n. 3/2018 (LOPDGDD) e le sue caratteristiche e funzioni rimanevano sostanzialmente immutate rispetto al GDPR, circostanza a cui fa da contrappeso l'introduzione di due importanti elementi di distacco, tanto dal Regolamento UE quanto dalla disciplina italiana: l'espresso richiamo normativo a certificazioni delle capacità professionali e la funzione di mediatore nell'utilizzo degli strumenti di ADR[54].

Il DPD è regolamentato dagli artt. 34-37 della *ley*, i quali disciplinano rispettivamente

di II livello "Data Protection Officer" patrocinato dal Garante per la Protezione dei Dati Personali, circostanza che dimostra una certa istituzionalizzazione del programma formativo.

[51] S. Comellini, *Il responsabile della protezione dei dati: Data Protection Officer DPO aggiornato al d. lgs. del 10 agosto 2018, n. 101 in materia di privacy*, cit., 38-39.

[52] *Real Decreto-ley* 5/2018*, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.*

[53] *Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales*. La *ley orgánica* può essere accomunata ad una legge rinforzata italiana, di cui è prescritto l'utilizzo solo per determinate materie ritenute particolarmente rilevati; così l'art. 81, comma 1 della Costituzione spagnola, che impone l'utilizzo delle leggi organiche per "la definizione dei diritti fondamentali e delle libertà pubbliche".

[54] Le *Alternative Dispute Resolution* sono strumenti di risoluzione della controversia alternativa alla giurisdizione che favoriscono la ragionevole durata del processo e contribuiscono all'alleggerimento del carico giudiziario affidando alle parti la risoluzione amichevole delle controversie tra loro insorte. Cfr. L. Montesano-F. De Santis-G. Arieta, *Corso Base di Diritto Processuale Civile*, Padova, 2019, 1041-1042.

la designazione, la qualifica, la posizione e l'intervento del *Delegado* in caso di reclamo all'Autorità di controllo.

L'art. 34 non apporta molto alla disciplina del Regolamento, ma ha il merito di provvedere all'elencazione di una serie di persone fisiche e giuridiche in ogni caso obbligate alla nomina di un DPD[55], attività svolta più minuziosamente dal legislatore rispetto alla realtà italiana, completata dall'opera del Garante più che dal legislatore. In virtù dell'esistenza delle Autorità di controllo regionali, poi, è prevista la comunicazione del suo nominativo nel termine di 10 giorni tanto alla Agencia Española de Protección de Datos quanto a quest'ultime, così come dev'essere comunicata loro ogni modificazione relativa alla figura, disposizione completata dal corrispettivo obbligo per le Autorità di conservare un registro aggiornato ed accessibile al pubblico.

Allo stesso modo, la posizione del DPD non viene ampliata dall'art. 36 rispetto alle disposizioni del Regolamento, ma questo si limita a specificare al par. 4 che qualora il Delegato rilevi un'importante lesione nella struttura in cui opera, dovrà documentare e comunicare immediatamente le sue valutazioni ai superiori gerarchici del titolare e responsabile del trattamento, compito facilmente desumibile dalla generica funzione di sorveglianza e dalla posizione d'indipendenza del DPD.

Totalmente nuovi, invece, sono gli artt. 35 e 37 della *ley orgánica*. Il primo fa riferimento alla possibilità di dimostrazione del possesso dei requisiti indicati dal par. 5, art. 37 del GDPR, affermando che è possibile sì utilizzare meccanismi volontari di certificazione, ma anche che questo è solo uno tra i possibili mezzi, fissando anche una certa libertà di forma. È probabilmente intenzione del legislatore disciplinarli più nel dettaglio nella (prossima) regolamentazione di attuazione.

Ebbene, l'Autorità di controllo spagnola ha redatto lo "Schema di certificazione dei Delegati alla protezione dei dati"[56] che mira a fornire uno strumento utile ad una valutazione oggettiva ed imparziale sulle qualità professionali dei DPD, a garanzia delle qualifiche e competenze dei futuri Data Protection Officers. Lo schema fornisce un modello di certificazione non obbligatorio che designa l'ENAC (*Entidad Nacional de*

[55] Vedi art. 34, par. 1: a) le scuole professionali ed i suoi consigli generali; b) i centri che offrono insegnamenti in qualunque livello; c) gli enti che prestano servizi di comunicazioni elettroniche quando trattino abitualmente e sistematicamente dati personali su larga scala; d) i prestatori di servizi della società dell'informazione quando elaborino su larga scala profili degli utenti del servizio; e) gli enti comprese nell'art. 1 della Legge 10/2014, di 26 di giugno, di ordinazione, supervisione e solvenza di entità di credito; f) gli stabilimenti finanziari di credito; g) le compagnie di assicurazione; h) le imprese di investimento regolamentate dalla legislazione della Borsa valori; i) i distributori di energia elettrica e di gas naturale; j) gli enti responsabili di archivi comuni per la valutazione della solvenza patrimoniale e del credito o per la gestione e prevenzione della frode; k) gli enti che sviluppano attività di pubblicità, includendo quelle di indagine commerciale e di mercati, quando causino trattamenti basati sulle preferenze degli interessati o realizzino attività che implichino la profilazione degli stessi; l) i centri sanitari legalmente obbligati al mantenimento delle storie cliniche dei pazienti, ad eccezione dei professionisti che, pure essendo legalmente obbligati al mantenimento delle storie cliniche dei pazienti, esercitino la propria attività a titolo individuale; m) gli enti che abbiano tra le proprie finalità la revisione contabile che possono riferirsi a persone fisiche; n) gli operatori che sviluppano attività di gioco attraverso canali elettronici, informatici, telematici ed interattivi; n) le imprese di sicurezza privata; o) le federazioni sportive quando trattano dati di minori di età.

[56] *Esquema de certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos (Esquema AEPD-DPD)*, in *aepd.es*.

Acreditación[57]) quale unico organismo per l'accreditamento degli Enti di certificazione (EC) che intendano partecipare allo Schema, i quali, a loro volta, offriranno la formazione adeguata al soddisfacimento dei requisiti del DPD[58]; anche le università, private e pubbliche, possono richiedere all'ENAC il riconoscimento dei propri programmi formativi forniti nella formula del Master.

Lo Schema riprende le competenze tecniche richieste dal Regolamento UE, meglio specificando quelle conoscenze, abilità o padronanze necessarie che possano attestare la rispondenza del candidato ai requisiti richiesti per svolgere la funzione di *Delegado de protección de datos*[59]. Lo Schema precisa anche che, oltre all'esperienza professionale, qualità personali quali l'integrità ed un elevato livello di etica professionale da garantire anche successivamente al rilascio dell'attestazione assumono una certa rilevanza[60]; procede poi con la determinazione delle modalità di valutazione, dei criteri di certificazione, dei diritti e doveri dei richiedenti e della gestione sui reclami relativi allo Schema stesso.

La AEPD è stata sicuramente antesignana nella predisposizione di una disciplina concreta sul DPD, atta a garantire un adeguato ed effettivo livello di competenze per tutelare al meglio i dati personali degli interessati, tuttavia condivido l'opinione di chi ritiene che, in quanto figura europea, il DPO dovrebbe godere di una regolamentazione generale affinché i requisiti e le qualifiche siano uniformi in tutti gli Stati membri. In caso contrario si verificherebbe nuovamente la produzione di un mosaico di discipline potenzialmente in contrasto tra loro come già nella vigenza della direttiva 95/46/CE, venendo così meno l'obiettivo di riforma generale perseguito. È dunque auspicabile una normativa omogenea in materia, eventualmente da predisporre attraverso la formalizzazione di una regolamentazione EN da parte degli organismi di controllo europei, generalmente dedita ad uniformare la normativa tecnica in tutta Europa[61].

Nondimeno ritengo che, sebbene la AEPD abbia disposto l'*Esquema AEPD-DPD*, la circostanza è controbilanciata dalla volontarietà del meccanismi di certificazione, infatti l'art. 35 della legge organica afferma che i requisiti del DPD «potranno essere dimostrati, tra gli altri mezzi, attraverso meccanismi volontari di certificazione che terranno particolarmente conto dell'ottenimento di un titolo universitario che accrediti conoscenze specializzate nel diritto e nella prassi in materia di protezione di dati», non escludendone altri differenti.

Altro rilevante elemento di novità e di distacco dal Regolamento UE e dal Codice italiano è la previsione dell'ulteriore funzione del DPD quale "strumento utile per la composizione amichevole dei reclami"[62]. Ai sensi dell'art. 37 della LOPDGDD, l'interessato può presentargli le richieste che non abbiano ottenuto riscontro positivo dal

[57] È l'entità designata dal Governo, in applicazione del Regolamento (CE) 765/2008 che regola il funzionamento dell'accreditamento in Europa, che opera in Spagna come l'unico Organismo Nazionale di Accreditamento; cfr. Portale *¿Qué es ENAC?* del sito ufficiale dell'Ente, in *enac.es*.

[58] Cfr. *Esquema AEPD-DPD*, cit., 2.

[59] Ivi, 5-7.

[60] Ivi, 8-9.

[61] M. Colombo, *Certificazione del DPO: occorre una norma europea (EN)*, in *privacydpo.org,* 27 luglio 2017.

[62] Cfr. *Preámbulo* della *Ley Orgánica* 3/2018.

titolare o dal responsabile del trattamento prima di rivolgersi all'Autorità di controllo nazionale o regionale, che il Delegato alla Protezione dei Dati dovrà evadere entro due mesi dalla ricezione. Qualora l'interessato ometta questa fase previa, anche la AEPD e le Autorità regionali adite potranno rimettere il reclamo al DPD affinché si esprima nel termine di un mese per poi, in assenza di riscontro, dar seguito al procedimento secondo le norme stabilite dal Titolo VIII della legge organica.

Altro profilo d'interesse riguarda la mancata abrogazione del *Real Decreto* 1720/2007 nonostante la meticolosa opera di armonizzazione, probabilmente da giustificare con la mancanza di un *reglamento de desarrollo* della nuova disciplina. Tale circostanza, però, può portare ad una parziale sovrapposizione della nuova figura del *Delegado* con quella del *Responsable de Seguridad* contemplata dal RLOPD del 2007. Come già esposto, il Responsabile della Sicurezza è designato per coordinare e monitorare le misure di sicurezza relative agli archivi contenenti dati personali che richiedano un livello di protezione medio o alto, mentre la nuova figura del Delegato alla Protezione dei Dati non coincide pienamente con questo infatti, sebbene entrambe siano legate alla sicurezza del trattamento dei dati, il regime giuridico delle figure differisce[63], così come il loro ambito materiale di applicazione. L'opera del DPD è certamente più ampia e riveste un ruolo chiave nella creazione di una *privacy policy* del designante, mentre il RS si limita al coordinamento e controllo su ciò che è già stato stabilito dal *Responsable del fichero*: mentre il Delegato si concentrerà, tra le altre funzioni, sull'analisi del rischio sui diritti e le libertà degli interessati (DPIA), il Responsabile della Sicurezza analizza i rischi relativi alle tecnologie utilizzate in concreto nelle attività di trattamento. Non tutti gli enti né i trattamenti, poi, richiedono la nomina di un DPD, motivo per cui la sopravvivenza della figura del Responsabile della Sicurezza non pare in contrasto con la nuova regolamentazione europea e, inoltre, i compiti attribuitigli possono servire da sostegno e contributo alle funzioni del DPD[64].

Sul tema, l'Agencia Española[65] ritiene che unificare i due soggetti in un'unica figura potrebbe generare un conflitto di interessi, causando il riversamento nella figura del *Delegado* sia dei compiti di garanzia della sicurezza dei dati, tipici del RS, sia delle funzioni di garanzia dei diritti e delle libertà degli interessati del Data Protection Officer; una completa sovrapposizione delle due figure potrebbe configurarsi solo eccezionalmente, qualora si tratti di un organismo pubblico che per le esigue dimensioni e le poche risorse non riesca ad ottemperare all'obbligo di nomina di un DPD.

Ritengo, tuttavia, che tale ordine di conclusioni non possa essere replicato in via generale: il compito del Data Protection Officer non si limita alla tutela dei diritti e delle libertà degli interessati, ma spazia sino a comprendere una pluralità di funzioni e competenze, motivo per cui si parla di "figura ibrida" e di "elemento chiave" della riforma operata dal GDPR. Sono chiari i compiti di vigilanza e controllo del DPO nei confronti di titolari e responsabili di ogni sorta, garantiti dall'indipendenza di cui il soggetto gode anche nel relazionarsi all'Autorità di controllo e per tali ragioni ritengo

[63] Vedasi il principio d'indipendenza sancito per il DPD, non previsto per il RS.

[64] R. Perales Cañete, *¿Bye bye Responsable de Seguridad, hello DPO?*, in *derechomásinformática.es*, 9 marzo 2017.

[65] *Informe 2018/170, Incompatibilidad entre la figura del Delegado de Protección de Datos del RGPD y el Responsable de Seguridad de la Información del Esquema Nacional de Seguridad*, 10-11 e 16, in *aepd.es*.

che potrebbe essere possibile, se non auspicabile in termini di risparmio economico – obiettivo esposto in varie circostanze, riunire entrambe le figure in un unico soggetto.

8. Conclusioni

Merita di essere sottolineato come l'impostazione complessiva del regolamento riveli una vocazione tendenzialmente globale del sistema europeo di *data protection* ma, nonostante la straordinaria portata innovativa del regolamento, la riforma non mantiene tutte le promesse di armonizzazione. È possibile, infatti, individuare una serie di settori nei quali è destinata a perdurare una situazione di disomogeneità normativa tra uno Stato membro e l'altro, in particolare in relazione al Data Protection Officer.
Dalla comparazione tra le legislazioni nazionali e quella comunitaria è emerso come la Commissione europea si sia ispirata quasi esclusivamente al modello tedesco di *privacy officer* nella redazione del regolamento 2001/45/CE: i requisiti professionali necessari alla nomina, l'obbligo dell'ente designante di fornirgli risorse adeguate, l'indipendenza del soggetto e la sua funzione di garanzia sul corretto adempimento della normativa appaiono esser stati ripresi *in toto* dalla disciplina tedesca, prevedendo una figura che avesse un ruolo di tipo consultivo accanto all'Autorità di controllo.
Il Regolamento del 2001 ha costituito un salto di qualità nella regolamentazione e nella definizione della figura, lasciando trasparire l'importanza che il DPO avrebbe dovuto avere nel panorama della tutela dei dati personali e la necessità di una regolamentazione generale che lasciasse scarso margine alle fonti secondarie o a regolamenti interni. Successivamente, all'altezza del GDPR, il legislatore ha reso la figura più eclettica, mediando tra modelli diversi e ottenendo come risultato una figura con un ruolo di sorveglianza e controllo particolarmente importanti in cui il rapporto con l'Autorità di controllo è più intenso, sino all'affermazione del DPO quale punto di contatto interno per l'Autorità garante e gli interessati.
D'altro canto, vi sono punti di criticità che riguardano i requisiti del DPO: il problema principale sarà reperire figure realmente professionali. Si è infatti segnalato come l'assenza di una compiuta disciplina comunitaria al riguardo possa portare ad un ritorno al mosaico di discipline esistenti prima della generale riforma del "Pacchetto protezione dati", pericolo dato dalla lacunosità della disciplina europea: alcuni Stati, come la Spagna, stanno provvedendo a dotarsi di una legittima disciplina nazionale relativa al Data Protection Officer, attività apprezzabile, ma potenzialmente lesiva dell'auspicato omogeneo livello di tutela richiesto dai Trattati dell'Unione Europea.
In conclusione, l'analisi del percorso legislativo che ha contraddistinto la figura del Data Protection Officer consente dunque di asserire che il legislatore europeo sia stato tanto proattivo quanto cauto nel disciplinarla e, al di là dell'entusiasmo per una riforma di così ampia portata e significato, non resta che attendere le prossime valutazioni della Commissione europea, per capire se in risposta alle dinamiche e alle sfide del web 2.0 si possa rispondere con un diritto alla protezione dei dati personali di seconda generazione, una *data protection* 2.0.