LIBER AMICORUM
PER
PASQUALE COSTANZO

GIANLUCA BELLOMO

CONTRIBUTO ALLA PROBLEMATICA DELLA NATURA GIURIDICA DEL "*DATA PROTECTION OFFICER*" (DPO)

26 MARZO 2020

CONSULTA ONLINE
PERIODICO TELEMATICO ISSN 1971-9892

Gianluca Bellomo
Contributo alla problematica della natura giuridica del "*Data Protection Officer*" (DPO)

SOMMARIO: 1. La costituzionalizzazione della *privacy*. – 2. Protezione dei dati personali nel Regolamento (UE) 679/2016 (GDPR). – 3. Il Responsabile per la protezione dei dati (DPO) come soggetto a rilevanza pubblica: a) istituzione. – 4. *Segue*: b) ruolo, funzioni e caratteristiche – 5. *Segue*: c) i compiti interni all'organizzazione – 6. *Segue*: d) il rapporto con il Garante: verso una "rete" globale della protezione dei dati personali? – 7. Per non concludere.

1. La costituzionalizzazione della privacy

Lo sviluppo tecnologico, che è stato portatore di un processo di globalizzazione economico-politica esponenziale, ha inciso in modo rilevante, in generale, sull'evoluzione del costituzionalismo[1], ed in particolare, sia sulla conformazione materiale dei diritti esplicitamente garantiti dalla Carta costituzionale, sia sull'affermarsi di nuove tipologie di diritto che in alcuni casi non si sarebbero potuti affermare senza l'avvento, oggi sempre più tumultuoso, proprio delle nuove tecnologie[2].

Con il passare del tempo e con l'apporto fondamentale delle Corti, da una parte si sono affermati così "nuovi diritti"[3] che non hanno un esplicito riconoscimento in Costituzione ma che comunque, con il passare del tempo e con l'evoluzione sociale, hanno trovato pieno riconoscimento nella costituzione materiale[4]; dall'altra, invece, diritti già costituzionalmente garantiti hanno trovato una

---

[1] Su cui cfr. P. COSTANZO, *Il fattore tecnologico e le sue conseguenze*, in ASSOCIAZIONE ITALIANA DEI COSTITUZIONALISTI (cur.), *Costituzionalismo e globalizzazione*, Atti del Convegno di Salerno 23-24 novembre 2012, Jovene, Napoli, 2014.

[2] Così, come rilevato in dottrina, alle libertà civili (diritti di prima generazione) e alle libertà positive (diritti di seconda generazione) si sono aggiunte altre categorie di diritti (di terza e di quarta generazione) non esplicitamente presenti in Costituzione ma rispondenti alle esigenze che si sono affermate, proprio a seguito della globalizzazione, spesso a livello sovrastatale. A riguardo, sempre dallo stesso A., è stato anche rilevato come l'elenco delle "generazioni" dei diritti «va modificandosi col mutare delle condizioni storiche, cioè dei bisogni e degli interessi delle classi al potere, dei mezzi disponibili per la loro attuazione, delle trasformazioni tecniche e così via», N. BOBBIO, *L'età dei diritti*, Torino, Einaudi, 1990, 9. Su tali tematiche v. *amplius*, *ex multis*, almeno F. MODUGNO, *I «nuovi diritti» nella giurisprudenza costituzionale*, Torino, Giappichelli, 1995; ma anche, S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, Laterza, 2004; e ID., *Tecnologie e diritti*, Bologna, Il Mulino, 2006; nonché F. PIZZETTI, *Dati e diritti nell'epoca della comunicazione elettronica*, *in* ID., *I diritti nell'era della rete*, Torino, Giappichelli, 2012.

Con riferimento alle nuove tipologie di diritti in dottrina si è anche parlato, suggestivamente, di diritti "svelati", in quanto figli delle nuove tecnologie di comunicazione di massa e solo grazie alle quali questi diventano materialmente esercitabili, su cui cfr. P. COSTANZO, *Avete detto "diritti digitali"?*, in *Tecniche normative*, 13.VII.2016, 7.

[3] Come noto nell'introduzione di "nuovi diritti" ci si è spesso riferiti in dottrina alla clausola prevista dall'art. 2 Cost., sulla cui natura di catalogo dei diritti con carattere aperto o chiuso però si sono scontrate varie teorie, così vi è stato: chi ha sostenuto che tale clausola consenta l'introduzione di nuovi diritti; chi ha ritenuto tale catalogo come chiuso o riassuntivo; e chi, invece, ha optato per un ruolo funzionale dei nuovi diritti finalizzato a garantire quanto già affermato dalla Costituzione, su cui cfr. G.F. FERRARI ET AL., *Diritto pubblico*, Milano, EGEA, 2019, 377-380. Ma anche circa il riconoscimento e la garanzia, dei nuovi diritti, v. almeno A. BARBERA, *Art. 2*, in G. BRANCA (cur.), *Commentario della Costituzione*, Bologna, Zanichelli, 1975, 53; A. BALDASSARRE, *Diritti inviolabili* (voce), in *Enc. giur. Treccani*, Roma, Treccani, 20 ss.; P. BARILE, *Diritti dell'uomo e libertà fondamentali*, Bologna, Il Mulino, 1984, 56; C. MORTATI, *Istituzioni di Diritto Pubblico*, Padova, Cedam, 1969, 949.

[4] Per costituzione in senso materiale (o effettivamente vigente) qui si vuole intendere quella nozione di costituzione che «coincide con le prassi e i principi sistematici fondamentali in base ai quali si configurano di fatto i modelli e i procedimenti organizzativi delle istituzioni sovrane (cioè degli organi e poteri che determinano l'indirizzo politico), e si dispiegano le relazioni materiali tra queste, e tra queste e i cittadini» (G. DI PLINIO, *Diritto pubblico dell'economia*, Milano, Giuffré, 1998, 107), ovvero quella che si evince «quando si ritenga possibile attribuire rango costituzionale (o per lo meno posizione sopraelevata rispetto alle leggi ordinarie) a norme non inserite nel testo, ma affidate alla legge, o ai regolamenti parlamentari o alla consuetudine, con funzione integrativa del testo medesimo» (C. MORTATI, *Costituzione (Dottrine generali)*, in *Enc. dir.*, XI, 1962, 169), in cui si può anche trovare una esaustiva ricostruzione dei possibili significati della distinzione concettuale tra costituzione formale e costituzione materiale; ma anche, più di recente, M.

nuova declinazione, proprio a causa dello sviluppo tecnologico che ha inciso sull'esercizio degli stessi da parte dei cittadini che, in molti casi, hanno assistito al dilatarsi della sfera di azione materiale di questi, ma, per converso e parallelamente, anche all'affacciarsi di nuovi rischi di lesione dei diritti e delle libertà fondamentali derivanti proprio dall'esistenza e dall'uso delle nuove tecnologie[5].

In tale contesto, così, hanno trovato riconoscimento una serie di diritti consacrati e materialmente declinati dall'azione della Consulta quali, a titolo esemplificativo, la tutela dell'ambiente, il diritto all'identità di genere e all'identità personale[6].

D'altra parte, vanno però segnalati anche "nuovi diritti" che si sono imposti attraverso l'azione del legislatore e della giurisprudenza nazionale ed europea e tra questi un esempio estremamente interessante è rappresentato proprio dalla tutela della privacy e dei dati personali. Tale ambito, infatti, essendo fortemente interconnesso e quindi influenzato dal progresso tecnologico, rappresenta un prezioso laboratorio per indagare i profili evolutivi del moderno costituzionalismo in ottica multilivello e nelle dinamiche giuridiche di influenza tra ordinamenti nello scenario globale, e quindi in definitiva del processo di c.d. "internazionalizzazione del costituzionalismo"[7]. Ciò sia con riguardo alla tutela dei diritti e delle libertà fondamentali che vengono specificamente in contatto con il tema della tutela dei dati personali; sia per l'inferenza sulle dinamiche generali che possono assumere i meccanismi ed i processi regolatori a livello sistemico globale[8].

Quando si parla di *diritto alla privacy* o più semplicemente di *privacy*, però, occorre preliminarmente riflettere sui confini concettuali che ne delimitano la nozione. Sempre più spesso,

---

DOGLIANI, *Costituzione in senso formale, materiale, strutturale e funzionale: a proposito di una riflessione di Gunther Teubner sulle tendenze autodistruttive dei sistemi sociali*, in *Costituzionalismo.it*, 3/2009.

[5] Si pensi a riguardo, ad esempio, all'espansione materiale che ha trovato l'art. 21 Cost. it. con la diffusione di massa dei *social network*, e parallelamente ai rischi derivanti tra gli altri dalle c.d. *fake news* o da possibili influenze sul corretto esercizio del diritto di voto veicolate proprio attraverso tali strumenti (sulle prime cfr. M. OROFINO, *Fake news e libertà di informazione*, in *MediaLaws*, 2/2018; ma anche il numero 1/2017 della stessa *Riv.* dedicato alla tematica; sulle seconde invece basti ricordare il recente caso *Cambridge Analytica* e le possibili influenze avute sulle elezioni presidenziali americane). A riguardo in dottrina è stato efficacemente affermato, anche se con specifico riferimento all'*e-government*, proprio circa i c.d. *diritti digitali*, come sia « … già possibile osservare come, più visibilmente rispetto ad altri fenomeni indotti dalla digitalizzazione dei segnali, l'*e-government* giustifichi che, dopo le varie generazioni di diritti che hanno accompagnato l'evoluzione dello Stato contemporaneo, si ragioni anche di "diritti digitali" (intendiamo utilizzare quest'espressione in senso diverso e più onnicomprensivo rispetto alla nota formula di *digital rights* invalsa nello specifico campo del diritto d'autore).

Si tratta – è vero – talvolta di risvolti di diritti e libertà tradizionali, ma ciò non toglie che si sia in presenza di una fenomenologia emersa solo grazie all'avvento del digitale. Per chiarire questa considerazione, può pensarsi al caso esemplare dell'emersione della privacy e, ancor prima, del diritto alla riservatezza: quest'ultimo correlabile a più di un diritto tradizionale, ma per così dire "svelato" di per sé solo con l'avvento della stampa di massa; e la prima, certamente implicata dalla libertà personale, ma percepita in via autonoma solo a seguito della capacità di archiviazione e di trattamento dimostrate dagli elaboratori elettronici.», P. COSTANZO, *Avete detto "diritti digitali"?*, cit., 7.

[6] Cfr. G.F. FERRARI ET AL., *Diritto pubblico*, cit., 378, ma anche, almeno, N. OCCHIOCUPO, *La Corte costituzionale tra norma giuridica e realtà sociale*, Bologna, Il Mulino, 1978; E CHELI, *Il giudice delle leggi*, Bologna, Il Mulino, 1996; F. MODUGNO, *La Corte costituzionale oggi*, in *Scritti in onore di Vezio Crisafulli*, Padova, Cedam, 1975.

[7] Su cui per approfondimenti cfr. M. RUOTOLO, *I diritti fondamentali, a settant'anni dall'entrata in vigore della Costituzione*, in *Diritto e Società*, I, 2018, 39-44.

[8] Un altro ambito che consente di indagare le dinamiche relative "all'internazionalizzazione del costituzionalismo", e che di fatto presenta caratteri molto simili a quelli che contraddistinguono la tutela della *privacy*, è rappresentato dal diritto pubblico dell'ambiente. Questo, infatti, non a caso si connota proprio per: la sua forte e diretta dipendenza dalla variabile dello sviluppo tecnologico, causa efficiente del fenomeno di globalizzazione e quindi del continuo mutare delle condizioni di operatività degli strumenti giuridici; l'incidenza diretta su valori giuridicamente riconosciuti dall'ordinamento come primari sia per i cittadini (es. diritto alla salute, diritto ad un ambiente salubre, ecc.), che per le future generazioni, come sancito ormai a tutti i livelli istituzionali dal ben noto principio internazionale dello «sviluppo sostenibile»; la pretesa di incidere su fenomeni che travalicano i confini nazionali ed i cui effetti negativi spesso si manifestano in ordinamenti giuridici differenti da quelli che li hanno originati (quando addirittura non producono effetti su scala globale). Infine il diritto pubblico ambientale, incidendo pesantemente e direttamente sui livelli di competitività dei soggetti economici a cui si rivolge negli odierni sistemi a base capitalistica, rappresenta un nuovo elemento strategico sempre più rilevante all'interno delle dinamiche che connotano il processo di trasformazione in atto nei mercati globali. Su cui sia consentito il rinvio a G. BELLOMO, *Le normazioni tecniche volontarie nel diritto pubblico dell'ambiente*, Napoli, Editoriale Scientifica, 2013, 1-221.

infatti, con tale termine ci si riferisce a beni giuridici o interessi spesso anche molto differenti tra di loro. Sovente, così, quando si parla di *tutela della privacy* si ha riguardo, in prima battuta, alla *tutela della riservatezza* in senso stretto, diritto ormai implicitamente riconosciuto dalla Carta costituzionale ed esplicitamente dall'art. 7[9] della Carta dei diritti fondamentali dell'Unione europea[10]. Tale accezione è sostanzialmente riconducibile alla tutela della propria vita privata da ingerenze esterne, ossia al c.d. "*Right to be let alone*" di origine statunitense[11]. Ma all'interno del concetto di *tutela della privacy* viene spesso ricompreso molto di più. La tutela della segretezza, dello spazio privato, la tutela dei propri dati personali[12], come peraltro esplicitamente disciplinato oggi nell'art. 8[13] della *Carta dei diritti fondamentali dell'Unione europea*.

Proprio la tutela della privacy e dei dati personali hanno trovato un primo importante riconoscimento a livello europeo già con l'adozione della Direttiva 95/46/CE, che, però, nasceva sostanzialmente con l'intento di funzionalizzare entrambi i diritti alla libera circolazione dei dati ed allo sviluppo del mercato interno. Solo in un secondo tempo, con l'adozione della *Carta di Nizza*, come ricordato, tali diritti hanno trovato un autonomo riconoscimento di natura costituzionale a livello europeo al quale è seguita, a colpi di sentenze della Corte di Giustizia[14], una decisa azione di *enforcement* e di contestuale delimitazione dei confini materiali degli stessi[15].

---

[9] *Articolo 7 - Rispetto della vita privata e della vita familiare.*

«Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni».

[10] Su cui per una ricostruzione sistematica v. S. SCAGLIARINI, *La riservatezza ed i suoi limiti*, Roma, Aracne, 2013, 91-123.

[11] Ovviamente ci si riferisce all'ormai noto articolo pubblicato il 15 dicembre del 1890 dai due giovani avvocati bostoniani che ebbe il merito di avviare la discussione negli USA sul riconoscimento di un diritto alla privacy, cfr. L.D. BRANDEIS, S. WARREN, *The Right of Privacy*, in *Harvard Law Revue*, 4/1890, 193-220. Per la verità, come rilevato in dottrina, già nel 1880 in Germania la tematica era stata introdotta, con meno fortuna mediatica, v. J. KHOLER, *Das Autorrecht, eine zivilistische Abhandlung*, in *Jering's Jahrbucher f. d. Dogmatik*, XVIII, Jena, 1880, 352 s., e dalla quale peraltro sembra plausibile che almeno Brandeis sia stato influenzato, considerati i suoi studi effettuali a Lipsia, come rilevato in R. PARDOLESI, *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, in R. PARDOLESI (cur.), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, Giuffrè, 2003, 4. Per una approfondita ricostruzione dell'evoluzione storico-giuridica del diritto alla riservatezza negli USA e in Europa cfr. anche M. SURACE, *Analisi socio-giuridica del rapporto tra sorveglianza e diritto alla riservatezza nell'era di Internet*, in *ADIR-L'altro diritto*, 2005, cap. 2.

[12] In tal senso cfr. G. FINOCCHIARO, *Riflessioni sul poliedrico Regolamento europeo sulla privacy*, in *Quad. cost.*, XXXVIII, n. 4, dicembre 2018, 895.

Va qui rilevato che proprio la tutela dei dati personali viene a configurarsi come lo strumento che, ove correttamente impiegato, si prefigge di garantire il fine della tutela della riservatezza e della privacy in un rapporto, quindi, di tipo funzionale.

[13] *Articolo 8 - Protezione dei dati di carattere personale*.

«1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la 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 persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.

3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

[14] Si pensi a titolo di esempio alle varie sentenze quali, sui periodi di conservazione dei dati personali *Digital Rights Irland*, C-293/12, (su cui cfr. L. TRUCCO, *Data retention: la Corte di giustizia si appella alla Carta dei diritti fondamentali dell'Unione europea e tutela vita privata e dati personali*, in *Giur. it.*, 2014, 1850-1856), ma anche più di recente, alle cause riunite C-203 e C-698/15, *Tele2 Sverige AB* (su cui cfr. F. GUELLA, *Data retention e circolazione dei livelli di tutela dei diritti in Europa: dai giudizi di costituzionalità rivolti alla disciplina UE al giudizio della Corte di giustizia rivolto alle discipline nazionali*, in *DPCE on line*, 2/2017, 349-357); *Schrems*, C-498/16, sul trasferimento di dati personali tra Europa e USA; *Google Spain*, C-131/12 sul diritto all'oblio e alla deindicizzazione da parte dei motori di ricerca (sulle quali *amplius* O. POLLICINO, *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, 14-26), ma anche *Google vs CNIL*, C507-17, che è recentemente tornata su quest'ultimo tema ridimensionando la portata della precedente sentenza (su cui sia consentito il rinvio a G. BELLOMO, *"Diritto all'oblio" e portata territoriale del "diritto alla deindicizzazione": la Corte ridisegna i confini applicativi*, in *DPCE on line*, 4/2019, 2987-2994).

[15] Su cui cfr. F. LATTUNEDDU, *L'ampliamento giurisprudenziale dei confini del diritto alla privacy*, in *Quad. dir. e pol. eccl.*, 3/2015, 943-966.

Infine, con l'approvazione 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[16], che ha abrogato la Direttiva 95/46/CE, si giunge alla definitiva costituzionalizzazione del diritto alla privacy e alla protezione dei dati personali in Europa[17].

2. *Protezione dei dati personali nel Regolamento (UE) 679/2016 (GDPR)*

Con la piena entrata in vigore del GDPR, se si è assistito ad un vero e proprio *tsunami* per le organizzazioni pubbliche e private che trattano dati personali, contestualmente però, si sono messi a sistema, all'interno di una norma generale comune di rango europeo, una serie di diritti, tutele ed istituti con rilevanti ricadute sui c.d. *interessati*[18].

Il Regolamento ha riscritto per tutti i Paesi membri la disciplina, originariamente introdotta con la Direttiva 95/46. Questo ha, quindi, rimodellato (ma in gran parte sostituito) la normativa italiana in materia abrogando tutte le norme statuite nel precedente Decreto legislativo 30 giugno 2003, n. 196 (c.d. *Codice della privacy*) incompatibili. Si è venuto così a positivizzare un nuovo rapporto nel bilanciamento tra diversi diritti fondamentali[19]. Contemporaneamente si è assistito, in Italia, alla convulsa azione di adeguamento, della normativa interna incompatibile, attraverso l'approvazione ed emanazione del D.lgs. 10 agosto 2018, n. 101[20].

Il Regolamento, insieme alle norme di adeguamento delle singole normative interne degli Stati membri, all'interno dei margini di azione da questo concessi, oggi, quindi, rappresenta uno dei modelli più avanzati, a livello globale, di tutela della privacy e dei dati personali[21].

---

[16] Entrato in vigore il 24 maggio 2016 e divenuto direttamente applicabile in tutti gli Stati membri già a partire dal 25 maggio 2018 (in seguito, secondo l'acronimo in lingua inglese, "GDPR" o Regolamento).

[17] Su cui cfr. G.F. FERRARI ET AL., *Diritto pubblico*, cit., 378 s.

[18] Per *interessato* si intende, come desumibile dallo stesso GDPR all'art. 4, 1), qualsiasi persona fisica identificata o identificabile alla quale sono riconducibili uno o più dati personali.

[19] Su cui v. C. DOCKSEY, *Four fundamental rights: finding the balance*, in *International Data Privacy Law*, 3/2016, Vol. 6, 195-209.

[20] A riguardo va evidenziato che il Legislatore italiano ha preferito, non senza critiche, percorrere la strada di modifica del pregresso *Codice della privacy*, invece di emanare un nuovo Codice che sostituisse il precedente. Ciò ha portato da una parte, forse, ad un passaggio di adeguamento meno traumatico per gli operatori coinvolti, ma dall'altra al *Codice della privacy* attuale che, quanto meno dal punto di vista del *drafting* normativo, risulta di non facile lettura. Si pensi solo, a titolo di esempio: da una parte all'art. 2 del Codice novato, che introduce ben sedici articoli dopo il due fino al 2-*septiesdecies*; e dall'altra all'abrogazione in sequenza di tutti gli articoli dal 3 fino al 45, oltre a molti altri nel prosieguo del testo in quanto incompatibili con il Regolamento, su cui per maggiori dettagli v. V. CUFFARO, *Quel che resta di un codice: il D.Lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del codice della privacy al regolamento sulla protezione dei dati*, in *Corr. giur.*, 10/2018, 1181-1185, che a riguardo ha efficacemente parlato di «intervento demolitorio».

Evidenza empirica, della confusione generata dalla scelta presa, è rinvenibile nel fatto che ancora oggi può capitare di leggere su documenti ufficiali o su moduli prestampati anche di pubbliche amministrazioni diciture che, nell'adeguare i richiami alle nuove normative introdotte in materia di privacy, richiamano esclusivamente il d.lgs. 101/2018, come se questo avesse abrogato, e non esclusivamente modificato, il precedente Codice del 2003.

[21] Il Regolamento si propone, così come conformato, come possibile *modello costituzionale mondiale per la tutela dei dati personali*, almeno nelle sue componenti fondamentali, verso il quale l'UE sembrerebbe essersi prefissa di far convergere gli altri modelli, ove presenti, negli ordinamenti extraeuropei. In tal senso si pensi, ad esempio, all'intero Capo V del GDPR che è dedicato al trasferimento di dati personali all'estero. Se il trasferimento di dati personali all'interno dell'UE, infatti, è sostanzialmente libero (dandosi per assunto che i soggetti coinvolti applichino correttamente le prescrizioni del Regolamento), quello verso i Paesi terzi, in assenza di idonee garanzie, e cioè di un livello di tutela dei dati personali che rispetti almeno i livelli minimi di tutela previsti dal modello europeo, è generalmente vietato. A riguardo il Codice prevede differenti livelli di deroga al generale divieto di trasferimento, modulati sull'idea che più il Paese terzo si adegua al *nucleo* della disciplina prevista a livello europeo e minori saranno i vincoli nel trasferimento dei dati coinvolti, ma con ogni probabilità anche dei relativi costi. Va però rilevato a riguardo che ove il modello europeo non dovesse trovare, almeno nei principi fondamentali la diffusione sperata, il rischio opposto potrebbe essere quello che la normativa adottata in UE per la tutela dei dati personali si possa trasformare in un *unicum* nello spazio globale che porti

A ben vedere, però, il Regolamento ha una portata di gran lunga più ampia rispetto ai confini normativi legati alla mera nozione di tutela della riservatezza, dettando disposizioni inerenti alla tutela dei dati personali anche quando questi ultimi non sono direttamente collegabili alla vita privata degli interessati, o ad aspetti di tipo strettamente personale[22].

Il Regolamento, già dalla denominazione, risulta portatore di un duplice livello di tutela da bilanciare e cioè: da una parte la protezione delle persone fisiche, con riguardo al trattamento dei dati personali; ma, dall'altra, cosa spesso ignorata, soprattutto in fase applicativa dello stesso, una maggiore libera circolazione di tali dati[23]. Il Regolamento, quindi, nasce sicuramente per tutelare le libertà ed i diritti fondamentali dei cittadini come prima *mission*, con particolare attenzione alla creazione di un modello di corretto trattamento dei dati personali che, posto in essere da parte delle organizzazioni che li gestiscono, possa ridurre il più possibile il livello di rischiosità di produzione di eventuali danni per i soggetti coinvolti[24]; dall'altra però, non si prefigge lo scopo di bloccare la circolazione dei dati personali, ma bensì di fornire un contesto normativo generale ed uniforme a livello europeo caratterizzato da maggiori margini di certezza, che consenta di coniugare queste due esigenze, favorendo al contempo un elevato livello di effettività nel perseguimento dei due obiettivi in una realtà sempre più tecnologizzata[25].

Ovviamente l'estensione formale e materiale dell'ambito di applicazione del Regolamento si gioca tutta sulla nozione di «dato personale»[26], che viene definito come «*qualsiasi 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,*

---

all'isolamento dell'Unione e quindi ad una contestuale diminuzione dei propri livelli di competitività nei regionalismi macroeconomici mondiali in continua trasformazione. Peraltro va anche rilevato che il ruolo della Corte di giustizia sta influendo e non poco sulla conformazione di tale modello e sui limiti di applicabilità dello stesso, si pensi a riguardo a quanto statuito in materia di diritto all'oblio e nello specifico circa il diritto alla deindicizzazione. Su tali dinamiche cfr. G. FINOCCHIARO, *Riflessioni*, cit., 897; ma anche, in particolare con riferimento al diritto all'oblio e alla sua evoluzione alla luce delle pronunce della Corte di giustizia v. O. POLLICINO, *Un digital right to privacy 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, 569-590, e più nello specifico ID., *Limitare il diritto all'oblio è un rischio*, in *Ilsole24ore*, 24 settembre 2019; e ID., *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale*, in *Federalismi.it*, 3/2014, 27.

[22] Così come affermato in dottrina «I dati personali costituiscono il tema disciplinato anche se non si riferiscono a vicende private, intime o familiari. 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.», G. FINOCCHIARO, *Riflessioni*, cit., 896.

[23] Un esempio di come il Regolamento cerchi di favorire la circolazione dei dati è rappresentato dall'introduzione del «diritto alla portabilità dei dati», previsto all'art. 20. Tale diritto sancito nel GDPR nasce proprio con l'intento di rimuovere quegli ostacoli che non consentono il rapido trasferimento dei dati di clienti tra operatori. Si pensi, ad esempio, ad un utente che intenda cambiare operatore telefonico o internet service provider. Troppo spesso, infatti, sono stati utilizzati presunti ostacoli al trasferimento di questi al fine di scoraggiare il passaggio da un fornitore di un servizio ad un altro creando di fatto delle distorsioni alla libera concorrenza tra operatori con conseguenze negative in particolare a carico dei consumatori.

[24] A riguardo va evidenziato che la tutela dei dati personali, potendo essere potenzialmente lesiva di diritti fondamentali in via diretta o indiretta, può essere considerata oggi a pieno titolo come *esercizio di attività pericolosa* posta in essere dal titolare del trattamento (o dal responsabile) ai sensi dell'Art. 2050 del codice civile con tutto ciò che ne consegue.

[25] Un esempio applicativo di tale tensione e di come non sia facile trovare un ragionevole bilanciamento nell'azione di *enforcement* della normativa in analisi può essere rappresentato dal contemperamento tra tutela della privacy e protezione dei dati personali, da una parte, e, dalla necessità di assicurazione un adeguato livello di sicurezza pubblica e di integrità del sistema finanziario europeo dall'altra, su cui per approfondimenti cfr. L. BORLINI, *Tutela della privacy e protezione dei dati personali a fronte della sicurezza pubblica e dell'integrità del sistema finanziario europeo*, in *Diritti umani e diritto internazionale*, 1/2017, 23-49.

[26] Collocata, significativamente, come prima definizione, al primo punto, del primo comma, dell'art. 4 del Regolamento relativo, appunto, alle definizioni.

genetica, psichica, economica, culturale o sociale». Ne consegue, quindi, che qualsiasi dato ricollegabile in via diretta o indiretta ad un soggetto fisico rientra nell'alveo della disciplina in parola[27]. Ma osservando il Regolamento da questa prospettiva, risulta evidente quanto la mera accezione di tutela della privacy, nel senso di tutela della riservatezza, risulti del tutto inadeguata a descrivere compiutamente la reale portata dell'ambito di operatività dello stesso. Così, invece, i concetti di privacy e di tutela dei dati personali, che il Regolamento si prefigge di garantire, coinvolgono, nell'ottica di quanto appena rilevato, anche molto più in generale, il regime di circolazione delle informazioni[28], in aree proprie di altri settori e materie, quali il mercato della concorrenza sulle informazioni e l'accesso alle informazioni[29].

Se a quanto rilevato si aggiunge che l'aumento esponenziale delle applicazioni tecnologiche e del loro uso sempre più necessita del trattamento di dati collegati o collegabili a soggetti fisici per consentirne l'utilizzo[30], risulterà chiaro come la portata del Regolamento e la relativa disciplina si stiano di fatto estendendo ben oltre il confine formale che ci si potrebbe rappresentare ad una prima lettura del campo di applicazione del GDPR, diventando di fatto onnipervasive[31].

---

[27] Da quanto previsto quindi i confini applicativi del Regolamento si estendono significativamente. Si pensi ad esempio alla mole di informazioni riconducibili a singoli soggetti in via diretta o indiretta ed indipendentemente dal fatto che queste informazioni siano strettamente personali o meno (es. la visita fatta da un utente ad un determinato sito web, la localizzazione di una persona in un dato posto, anche quando questa localizzazione possa essere fatta in via indiretta e non immediata e così via).

Sempre sulla nozione di dato personale va inoltre segnalato l'enorme problema legato alla deduzione di dati personali da dati che inizialmente non lo erano. Si pensi, a titolo di esempio, a come in alcuni casi con il ricorso a tecniche di analisi dei Big data si possa risalire ad informazioni personali; all'accesso illecito, magari per via informatica, a banche dati che consentano di de-pseudonimizzare dati che solo inizialmente erano classificabili come personali; ma ancora a tutta la problematica dell'uso dei programmi di intelligenza artificiale ed ai dati personali che potrebbero trovarsi a trattare nell'esercizio delle funzioni a queste assegnate. Su cui per ulteriori approfondimenti v. T. TANI, *L'incidenza dei big data e del machine learning sui principi alla base del Regolamento Europeo per la tutela dei dati personali (2016/679/UE) e proposte per una nuova normativa in tema di privacy*, in S. BONAVITA (cur.), *Società delle tecnologie esponenziali e General Data Protection Regulation*, Torino, Ledizioni, 35-65.

[28] Peraltro, come è stato affermato in dottrina, «il dato personale è l'oggetto del diritto fondamentale riconosciuto dall'art. 8 della Carta europea dei diritti fondamentali. Quando i dati costituiscono oggetto di scambio, si profila quindi un contrasto fra la realtà commerciale internazionale e la concezione teorica tradizionale che afferma l'indisponibilità dei diritti della personalità. Anche il paradigma proprietario appare inadeguato: i dati personali non sono oggetto di un diritto esclusivo, ma sono invece oggetto di fruizione da parte di una pluralità di soggetti. La medesima informazione, infatti, viene utilizzata da più soggetti per scopi e finalità diverse, su basi giuridiche differenti. Non si configura dunque un diritto di disporre in modo pieno ed esclusivo, ma piuttosto un diritto di utilizzo», G. FINOCCHIARO, *Riflessioni*, cit., 896 s.

[29] Su cui per approfondimenti, anche con specifico riferimento al ruolo in materia del Responsabile per la protezione dei dati personali cfr. G. RESTA, *Digital platforms and the law: contested issues*, in *MediaLaws*, 1/2018, 231-248.

[30] Tale concetto ovviamente va inteso in senso ampio. Infatti, svariate applicazioni potrebbero funzionare, tecnicamente, anche senza la raccolta di dati personali, ma l'inserimento obbligatorio per il loro utilizzo da parte degli utenti, in molti casi, viene utilizzato per consentire allo sviluppatore dell'applicazione di monetizzare il lavoro posto in essere. Proprio la cessione a terzi di dati personali raccolti grazie all'uso dell'applicazione informatica, così, diventa l'elemento che consente di avere una sostenibilità economica nel tempo dell'applicazione. L'alternativa principale è rappresentata dal pagamento di una somma per l'uso dell'applicativo d'interesse. In buona sostanza, sempre più spesso, nel mercato digitale paghiamo la fruizione di un servizio con la cessione dei nostri dati personali. Ciò, va rilevato, accade anche al di fuori della Rete: si pensi, ad esempio, a quando, facendo un acquisto in un negozio, arrivati alla cassa, ci viene proposto di sottoscrivere una tessera fedeltà, con la quale di fatto cediamo nostri dati personali, a fronte di una percentuale di sconto sull'acquisto che stiamo per effettuare. In quest'ultimo caso possiamo quantificare esattamente la valutazione fatta in quel momento dal mercato dei dati personali che sono stati richiesti.

[31] Su cui cfr. C. TITO, *Perché la democrazia oggi è fondata sulla nostra privacy*, in *La Repubblica*, 18 giugno 2018, 1-2, che, riprendendo le dichiarazioni di Antonello Soro, attuale presidente in proroga dell'autorità Garante per la Privacy, efficacemente riassume «L'espansione di internet e dei social media sta avendo un impatto non solo sugli stili di vita di tutti i cittadini del mondo, ma anche sulla qualità delle nostre democrazie.

C'è un elemento che appare sempre più di inestricabile difficoltà con la crescente penetrazione del web nelle abitudini di ognuno di noi: il controllo dei dati che ci riguardano e la loro conservazione protetta. Le nostre abitudini, il tipo di lavoro, il modello di tempo libero che viene scelto costituisce una ricchezza per chiunque abbia bisogno di investire in qualsiasi settore.

Ma rappresenta soprattutto la più grande miniera per estrarre dalla popolazione il consenso. Ossia il voto e con esso quindi il successo elettorale. Un aspetto che ha già condizionato le campagne elettorali in molti paesi del mondo e anche

Ma quali sono gli elementi ed i principi che rappresentano il nocciolo duro del Regolamento e che potrebbero costituire, ove si affermassero, quel *common core* che il modello europeo di tutela della privacy e dei dati personali sta cercando di imporre a livello globale? Tra i più rilevanti si possono segnalare, ad oggi: il *principio di liceità* del trattamento dei dati personali, con particolare attenzione al requisito ed alla disciplina del *consenso*, in particolare del minore; il *principio di minimizzazione* nel trattamento di dati personali; il *principio di trasparenza* e *correttezza*; il *principio di conservazione* dei dati personali; il *principio di riservatezza* ed *integrità* dei dati personali; il *"diritto all'oblio"*; il *principio di accountability*; la *privacy by design* e *by default*; i profili di responsabilità[32].

3. *Il Responsabile per la protezione dei dati (DPO) come soggetto a rilevanza pubblica: a) istituzione*

Il GDPR, per quanto riguarda i soggetti coinvolti nell'applicazione del Regolamento, tra le novità di maggior rilievo, ha istituito, dedicandogli l'intera sezione 4, agli articoli 37, 38 e 39[33], la figura del *Data Protection Officer* ("DPO")[34], tradotta nella versione italiana del Regolamento con la locuzione di Responsabile della Protezione dei Dati ("RPD")[35].

---

in Italia. La possibilità di modellare la comunicazione e di tarare la propaganda sui singoli votanti è la prima conseguenza e, in una certa misura, anche la più lecita. Ma nelle distorsioni della rete è maturata – ed è ormai evidente – una seconda conseguenza: quella di determinare la scelta attraverso bisogni o paure indotte da messaggi continui e senza controllo sui social».

[32] Sui quali per maggiori approfondimenti cfr. almeno: G. FINOCCHIARO (dir.), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017; L. BOLOGNINI, E. PELINO, C. BISTOLFI (curr.), *Il Regolamento Privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, Giuffrè, 2016; S. SICA, V. D'ANTONIO, G.M. RICCIO (curr.), *La nuova disciplina europea della privacy*, Milano, Wolters Kluwer, 2016; i due tomi di G. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, *I (dalla dir. 95/46 al nuovo regolamento europeo)* e *II (Il regolamento europeo 2016/679)*, Torino, Giappichelli, 2016; G.M. RICCIO, G. SCORZA, E. BELISARIO (curr.), *GDPR e normativa privacy. Commentario*, I Ed., Milano, Wolters Kluwer, 2018; F. DE STEFANI, *Le regole della privacy. Guida pratica al nuovo GDPR*, Milano, Hoepli, 2018; G. FINOCCHIARO (dir.), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 2019; inoltre tra gli articoli cfr. A. SPINA, *Alla ricerca di un modello di regolazione per l'economia dei dati. Commento al regolamento (Ue) 2016/679*, in *Riv. regol. merc.*, 2016, 143 ss.; E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contratto e impresa*, 1/2018, 106-125; C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, 22/2018, 1-34.

[33] Rispettivamente, Articolo 37 «*Designazione del responsabile della protezione dei dati*»; Articolo 38 «*Posizione del responsabile della protezione dei dati*»; Articolo 39 «*Compiti del responsabile della protezione dei dati*».

[34] In realtà figure analoghe erano già presenti in alcuni ordinamenti europei tra cui quello tedesco (fin dal 2003) ed austriaco, come obbligatorie; ed in quello francese, invece, come facoltativa.

[35] D'ora in poi si userà l'acronimo inglese, sia perché facilmente riconoscibile in tutta Europa, ma soprattutto per evitare gli equivoci ai quali purtroppo si presta il termine italiano, dal momento che la traduzione di *Data Protection Officer* in *Responsabile per la Protezione dei Dati [personali]* non sembra essere stata delle più felici. Infatti il termine *responsabile* utilizzato per tradurre l'inglese *officer* ha creato non pochi problemi. Ciò sia con riferimento ad altre figure previste dallo stesso Regolamento quali, ad esempio, il *Responsabile del trattamento*, *ex* art. 28, così come con la precedente figura prevista dal previgente Codice privacy di *responsabile del trattamento "interno"* ex art. 29, oggi superata; ma anche dal punto di vista della possibile interpretazione del termine "*responsabile"* nel senso di una possibile imputazione, in capo a questo soggetto, di una specifica responsabilità nel caso di una non corretta applicazione del Regolamento all'interno dell'organizzazione di riferimento. Tale ultima ipotesi, dopo le prime incertezze, è stata ormai ampiamente risolta in senso negativo: infatti in caso di comminazione di sanzioni il soggetto che risponde per la non corretta gestione del *sistema privacy* sarà il titolare del trattamento (e quindi nemmeno il rappresentante legale) dei dati personali, e ciò proprio in considerazione del fatto che egli è l'unico a poter incidere materialmente sulla conformazione organizzativa interna e che quindi avrà l'ultima parola in termini di predisposizione e gestione del *sistema privacy* dell'organizzazione della quale rappresenta l'organismo di vertice. Questo, anche in caso di dissenso con il DPO, che giova ricordare non gode di poteri gestionali diretti interni all'organizzazione. Così il DPO non potrà essere direttamente responsabile civilmente rispetto a terzi e tanto meno potranno essergli imputate sanzioni amministrative che ricadranno esclusivamente sul titolare, unico responsabile dell'organizzazione e del funzionamento del *sistema privacy* interno all'organizzazione. Eventuali profili di responsabilità tra i due rileveranno solo ed esclusivamente con riferimento al

4. Segue*: b) ruolo, funzioni e caratteristiche*

L'introduzione della figura del DPO, precedentemente sconosciuta all'ordinamento italiano, ha creato, in questa prima fase applicativa del GDPR, non pochi dubbi interpretativi sulla precisa definizione del ruolo e delle funzioni che materialmente questa debba assumere rispetto al soggetto presso il quale è chiamata a svolgere il proprio incarico e nel rapporto con altri soggetti pubblici e privati. Se tale figura, infatti, ad una prima lettura del Regolamento, potrebbe sembrare connotarsi per una natura di tipo prettamente privatistica in quanto soggetto, interno o esterno all'organizzazione di riferimento, contrattualizzato per svolgere determinate funzioni, a ben vedere può assumere, ed in alcuni casi assume, una significativa rilevanza pubblica, sotto un profilo materiale, nell'esercizio delle funzioni a questa assegnate.

Per una corretta lettura delle funzioni e del ruolo di tale figura non si può prescindere dal fatto che il Regolamento prevede che il DPO sia un soggetto necessariamente designato[36] in tutte le organizzazioni pubbliche ed in quelle private nelle quali, in buona sostanza, i trattamenti dei dati personali potrebbero comunque presentare rilevanti livelli di rischiosità per i dati personali trattati ed, in ultima istanza, per la tutela dei diritti e delle libertà fondamentali dei soggetti coinvolti[37]. Ne consegue che l'obbligo di nomina e la natura stessa dell'organizzazione all'interno della quale il DPO svolge le proprie funzioni possano influire anche significativamente sull'esercizio materiale dei compiti a questo assegnati, in particolare nel rapporto con le relative finalità di rilievo giuspubblicistico[38].

---

rapporto contrattuale assunto e quindi presumibilmente in caso di palese omissione o errata indicazione data dal DPO al titolare sul corretto adeguamento dell'organizzazione alle norme in materia. D'altra parte ove fosse possibile poter scaricare la responsabilità personale, da parte del titolare, sul DPO, e quindi separare la prevista responsabilità dai poteri gestionali e organizzativi interni, si creerebbe un *vulnus* enorme nel realistico perseguimento delle tutele previste dal Regolamento ed un inaccettabile indebolimento nell'azione di *enforcemnt* alla corretta implementazione e gestione del *sistema privacy* all'interno dell'organizzazione, con conseguente aumento, in ultima istanza, della rischiosità per i diritti e le libertà fondamentali degli interessati.

[36] Il Regolamento all'art. 37 «Designazione del responsabile della protezione dei dati» prevede che:

«1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure

c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.»

[37] Così il Regolamento prevede l'obbligatorietà di designazione quando il titolare attua un «monitoraggio regolare e sistematico degli interessati su larga scala» o nel caso in cui vengano trattate particolari categorie di dati personali (cioè che in buona sostanza presentano un livello di rischiosità per i diritti e le libertà degli interessati particolarmente alto ove non venissero trattati correttamente) su *larga scala*. Cosa intenda il Regolamento per *larga scala* però non viene esplicitato, lasciando così margini di incertezza su chi, tra i soggetti privati sia obbligato o meno a dotarsi di un DPO. Il Regolamento sembrerebbe cercare di applicare un principio di *efficienza* regolativa, infatti: proprio i soggetti privati rientranti nel concetto di *larga scala* sono quelli che potrebbero danneggiare un elevato numero di interessati nel trattamento dei propri dati personali; l'estensione dell'obbligo di designazione del DPO anche alle piccole imprese sarebbe difficilmente sostenibile economicamente da queste che rischierebbero di dover sopportare costi eccessivi; ma anche, con tale soluzione, la stessa figura del DPO viene valorizzata riservando, anche se nulla vieta una eventuale designazione volontaria della stessa anche da parte di chi non vi sia obbligato, l'esercizio di tale attività a soggetti con elevata qualificazione professionale e che quindi meglio possono incidere nella effettività dell'applicazione del Regolamento proprio in quelle organizzazioni dove maggiori sono i rischi per la corretta gestione dei dati personali. Su cui cfr. G.M. RICCIO, *Data Protection Officer e altre figure*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (curr.), *La nuova disciplina europea della privacy*, cit., 52.

[38] Un ulteriore elemento di riflessione e di futuro approfondimento attiene alle funzioni, e all'esercizio delle stesse, assegnate al DPO a seconda del soggetto presso il quale svolge la propria funzione. Infatti tale contesto lavorativo non

Le stesse caratteristiche che dovrebbe avere un DPO sono indicative dello stretto rapporto che questa figura ha, nell'esercizio dei compiti assegnati dal Regolamento, con la tutela dei diritti e delle libertà fondamentali. Infatti, nonostante non vi sia una esplicita previsione a riguardo, ormai sembra assodato che debba avere, *in primis*, ma non esclusivamente, una consolidata formazione giuridica[39] che gli consenta di gestire correttamente le norme di riferimento e soprattutto di effettuare nel migliore dei modi, anche grazie ad una sviluppata sensibilità riguardo alla tutela dei diritti, proprio quel necessario bilanciamento tra i valori costituzionali di volta in volta toccati dalle singole situazioni di applicazione della normativa in materia nelle quali si vede coinvolto. Il Regolamento che ha introdotto la figura del DPO nell'ordinamento europeo, come già ricordato, non può prescindere, infatti, dalla contemperazione dei due obiettivi che si prefigge: tutela dei dati personali da una parte e libera circolazione degli stessi dall'altra. Proprio del corretto bilanciamento tra queste due tensioni (anche in rapporto ad altri ulteriori diritti di rango costituzionale), di cui è portatore il Regolamento, si dovrà fare interprete il singolo DPO nello svolgimento dei compiti a lui assegnati, ma tale operazione dovrà essere sempre effettuata avendo ben chiare le possibili conseguenze derivanti, in ultima istanza, dalle scelte poste in essere dai singoli titolari per i diritti e le libertà fondamentali degli interessati. Ciò andrà fatto in particolare valutando attentamente il singolo contesto applicativo e gli strumenti a disposizione dell'organizzazione coinvolta, sempre con un approccio funzionalista e non meramente formalista, per il perseguimento delle finalità previste dal legislatore. Tale azione ermeneutica sulle norme e sui diritti, oltre che la valutazione dei rischi di contesto, di volta in volta interessati, richiede una chiara conoscenza, una visione ampia ed una sviluppata sensibilità *in primis* proprio nei confronti dei valori costituzionali formali e materiali coinvolti, e dei quali diventa quindi portatore il DPO, in particolare nella fase applicativa della normativa di riferimento[40].

Le considerazioni, qui ancora solo appena accennate, dovrebbero iniziare a far intuire l'importanza di una corretta enucleazione della esatta portata del ruolo e dei compiti minimi del DPO, all'interno

---

sarà ininfluente circa le modalità di esercizio dei propri compiti. 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).

[39] In tal senso già il Regolamento all'art. 37, c. 5, che prevede «Il responsabile della protezione dei dati è designato 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 di cui all'articolo 39», su cui cfr. A. CILONA, *I requisiti per la nomina del Data Protection Officer e la certificazione Lead Auditor ISO 27001*, nota a Tar Friuli-Venezia-Giulia, 13 settembre 2018, n. 287, in *MediaLaws*, 1/2019, 240-247.

[40] Si pensi, a riguardo, al difficile banco di prova costituito dal necessario contemperamento tra tutela della salute collettiva e tutela dei dati personali che si pone in queste dure giornate nell'affrontare i profondi cambiamenti richiesti dalla generale riorganizzazione, nel trattamento dei dati personali, attuata da parte delle organizzazioni a seguito dei cambiamenti imposti dalla pandemia legata alla diffusione del Coronavirus COVID-19 in Italia. Sia qui consentito solo accennare all'emanazione del recentissimo DL 9 marzo 2020, recante «*Disposizioni urgenti per il potenziamento del Servizio sanitario nazionale in relazione all'emergenza COVID-19*», che prevede all'art. 14 «*Disposizioni sul trattamento dei dati personali nel contesto emergenziale*»: al comma 3, alcune deroghe esplicite alle regole ordinarie di trattamento dei dati personali, ma contemporaneamente, anche in questa drammatica fase emergenziale, ribadisce l'obbligo del rispetto dei principi basilari del GDPR, così come sanciti all'art. 5; ma anche, al comma 6, la necessità che al termine di questa fase i trattamenti effettuati vengano ricondotti all'ambito delle ordinarie competenze e delle regole che disciplinano la materia, su cui anche su altri temi si è espresso direttamente il *Comitato europeo per la protezione dei dati – EDPB –* il 19 marzo 2020, con l'adozione della «*Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19*», pubblicata in italiano sul sito del Garante il 20 marzo. Sullo specifico tema, inoltre, con impostazione più netta, cfr. A. MONTI, *COVID-19: fuorilegge l'app che traccia gli utenti?*, in *ICT LEX*, Blog di Diritto, politica e cultura della Rete, 22/03/2020.

del modello europeo di tutela dei dati personali, proprio per garantire un elevato livello di garanzia degli interessati, e al contempo anche di corretta circolazione dei dati personali. Una interpretazione del ruolo e dei compiti a questo assegnati, incentrata esclusivamente su una applicazione formalista del Regolamento e non strettamente funzionale al perseguimento dell'obiettivo di perseguire una elevata tutela dei dati personali, infatti, può portare ad una applicazione della normativa in materia eccessivamente restrittiva che potrebbe ledere la corretta circolazione dei dati personali. Potrebbe, inoltre, far vivere gli adempimenti legati alla tutela di questi come un mero vincolo alle attività poste in essere da un'organizzazione e produrre, essa stessa, una condizione materiale non meno lesiva dei diritti e delle libertà dei cittadini[41]. All'estremo opposto, un bilanciamento attuato da un DPO che sia eccessivamente sbilanciato sulla circolazione dei dati personali potrebbe fargli perdere di vista proprio quelle libertà e quei diritti fondamentali che invece il legislatore europeo ha voluto riportare in primo piano in particolare nelle attività legate all'economia digitale, ma che non possono prescindere da un adeguato livello di raggiungimento della primaria finalità del Regolamento.

In buona sostanza, quindi, per comprendere fino in fondo il punto di vista del DPO nell'esercizio del proprio ruolo, e quindi dei propri compiti, si può assumere che questo deve fungere, da una parte, da portavoce qualificato dei diritti degli interessati all'interno delle organizzazioni che hanno l'obbligo o decidono di designarlo, sia nell'ottica, in ultima istanza, della riduzione dei livelli di rischiosità per i diritti e le libertà fondamentali di questi, ma anche in quella di favorire e agevolare la libera circolazione dei loro dati personali alle condizioni previste dalla normativa. Dall'altra, però, tale funzione non va assolutizzata, infatti, il DPO, ove dovesse trovarsi di fronte al contemperamento tra gli anzidetti diritti ed altri, comunque che presentino valenza di rango costituzionale ugualmente legittimi ma nel caso specifico preponderanti, dovrà senz'altro rappresentare fedelmente al titolare la sua visione, in base alla normativa vigente, circa la gerarchia di tutela che si dovesse venire a configurare tra questi con piena terzietà ed indipendenza. Da ciò dovrebbe risultare chiara l'imprescindibile necessità, per una corretta applicazione del quadro normativo in materia, che il DPO sia portatore di una chiara visione sistemica dell'ordinamento, che solo una formazione giuridica specialistica può fornire.

Se la lettura del ruolo del DPO viene fatta alla luce del fatto che il Regolamento assume sempre più, come rilevato, natura onnipervasiva, diventa ancora più evidente che la presenza del DPO nella corretta gestione ed applicazione delle disposizioni in materia di tutela dei dati personali riveste un ruolo di primo piano agli occhi del giuspubblicista, anche in ottica multilivello, proprio nel garantire e bilanciare i diritti e le libertà fondamentali di volta in volta coinvolte[42].

Proprio per consentire al DPO di svolgere correttamente il proprio ruolo all'interno delle organizzazioni coinvolte, il Regolamento prevede una chiara posizione[43] di questo rispetto al *titolare*, al *responsabile del trattamento*[44] ed agli *interessati*. Così il DPO: deve essere tempestivamente ed

[41] Infatti anche la mancata circolazione o accesso a dati personali può essere fortemente lesiva di diritti e libertà degli interessati. Un esempio di scuola sta diventando il mancato accesso o l'indisponibilità di dati sanitari per un medico che si trovasse a dover prendere decisioni, ad esempio di tipo terapeutico salvavita, su di un interessato (es. indisponibilità, anche temporanea, di accesso ad una cartella sanitaria elettronica).

[42] Su cui per alcuni primi approfondimenti in particolare nel bilanciamento tra privacy, protezione dei dati, libertà di espressione e trasparenza, cfr. C. DOCKSEY, *Four fundamental rights*, cit., 195-209.

[43] Articolo 38 «*Posizione del responsabile della protezione dei dati*».

[44] Per «*responsabile del trattamento*» si intende «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento», ex art. 4, c.1, 8), tale figura è poi disciplinata in dettaglio all'art. 28 del GDPR. L'introduzione di questa da parte del GDPR ha creato non poca confusione già solo in relazione alla presenza, nel previgente *Codice privacy*, nel soppresso art. 29, come già ricordato sopra, della figura del Responsabile "interno" del trattamento, che quindi oggi è stata superata a favore di questa nuova nozione che riguarda solo ed esclusivamente soggetti esterni all'organizzazione del titolare. Ma il richiamo al *responsabile del trattamento* può creare confusione anche da un altro punto di vista, giacché il titolare del trattamento nello svolgere le proprie attività nel rapporto con altri soggetti esterni può assumere come medesimo soggetto, ai fini della normativa privacy, a volte il ruolo di titolare autonomo nel trattamento dei dati, ma in altri casi può esso stesso assumere il ruolo, appunto, di *responsabile del trattamento*. In base a questa precisazione dovrebbe quindi risultare chiaro che il DPO, che opera all'interno di una organizzazione può essere chiamato a svolgere la propria funzione sia nei confronti del titolare di una organizzazione,

adeguatamente coinvolto[45] dal titolare in tutte le questioni relative alla protezione dei dati personali, in modo tale da poter fornire il proprio supporto specialistico nelle decisioni da prendere; dovrà essere supportato (tecnicamente ed economicamente) dal titolare, messo in condizione di svolgere le proprie funzioni e mantenere la propria formazione specialistica aggiornata[46]; nell'esercizio del proprio ruolo gode di una specifica tutela interna, infatti gli dovrà essere garantita la terzietà ed indipendenza rispetto ad eventuali interferenze del titolare (ma anche del responsabile del trattamento), si dovrà relazionare ai vertici dell'organizzazione ai quali riferirà sulle questioni nelle quali è coinvolto e non potrà essere discriminato o danneggiato, a maggior ragione se interno, a causa dei pareri o delle azioni poste in essere nell'esercizio dei propri compiti[47]; può essere contattato dagli interessati per questioni legate alla presunta violazione delle norme relative al trattamento dei propri dati personali causate dall'organizzazione nella quale è stato designato o relativamente all'esercizio dei diritti derivanti dal Regolamento[48]; avrà diritto di pieno accesso ai dati personali trattati dall'organizzazione nell'esercizio dei propri compiti e, per converso, un obbligo di segretezza o di riservatezza circa l'adempimento dei propri compiti nel rispetto del diritto dell'Unione o dei singoli Stati membri[49]; potrà svolgere, infine, ulteriori compiti e funzioni purché non in conflitto di interessi con l'attività da porre in essere presso l'organizzazione nella quale svolge il proprio incarico[50].

5. Segue*: c) i compiti interni all'organizzazione*

L'articolo 39[51] del GDPR prevede i *compiti* minimi da assegnare al DPO, ma ciò non vuol dire, che in fase di designazione il titolare non possa decidere di affidare a questo ulteriori compiti, che però andranno dapprima concordati con il DPO, quindi formalizzati e, ove comportino un aggravio lavorativo, remunerati. Il primo compito che il Regolamento richiede di svolgere al DPO è relativo alla *informazione* e *consulenza*[52] da fornire al titolare del trattamento, al responsabile del trattamento[53], nonché ai dipendenti che operano sui dati personali per quanto attiene agli obblighi del Regolamento, ma anche ad altre disposizioni in materia di tutela dei dati personali. All'interno di tali

---

sia, quando la medesima organizzazione assume il ruolo di responsabile del trattamento nei confronti di altri soggetti terzi, nei confronti di quest'ultimo. Ne consegue che quando la normativa si riferisce a tale figura non sta parlando di un altro soggetto terzo rispetto all'organizzazione che lo ha designato ma sostanzialmente del medesimo soggetto che assume ruoli e responsabilità diverse a seconda della tipologia di trattamento posta in essere.

[45] Art. 38, «1. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali».

[46] Art. 38, «2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica».

[47] Art. 38, «3. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento».

[48] Art. 38, «4 Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento».

[49] Art. 38, «5. Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri».

[50] Art. 38, «6. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi».

[51] Articolo 39 «*Compiti del responsabile della protezione dei dati*».

[52] Art. 39, «1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti: a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati».

[53] E cioè del medesimo titolare quando assume il ruolo di *responsabile del trattamento* rispetto ad altri soggetti, cfr. *supra* nt. 45.

specifiche funzioni, quindi, si esplica un ruolo rilevante del DPO che deve sia rendere edotto il titolare, *in primis*, ma anche l'intera organizzazione, sugli adempimenti previsti dal Regolamento (anche con opportuni aggiornamenti specificamente riferibili alle attività poste in essere dall'organizzazione); sia svolgere attività di *consulenza* e cioè, ove richiesto, di fornire il proprio punto di vista sull'applicazione della normativa in materia a casi concreti. Proprio in quest'ultimo caso il DPO è chiamato maggiormente ad adattare alle singole questioni a lui sottoposte l'applicazione dei criteri, esplicitandoli, in base ai quali effettuare il materiale bilanciamento nella tutela dei vari diritti costituzionalmente garantiti dalla normativa e coinvolti[54].

Un altro basilare compito assegnato al DPO attiene alla *sorveglianza sull'osservanza del Regolamento*[55] (e delle altre disposizioni in materia) con particolare riguardo alle relative scelte effettuate dal titolare (e dal responsabile). Queste ultime vanno intese in senso molto ampio, e cioè comprensive dell'attribuzione delle responsabilità, della sensibilizzazione e della formazione di tutti i soggetti che a vario titolo trattano dati personali all'interno dell'organizzazione di riferimento o sono connessi all'attività di controllo. Proprio tale compito, che tipicamente rientra tra quelli di un *officer*, cioè di un soggetto che in modo sistematico cerca di monitorare il funzionamento del sistema privacy del quale, all'interno dei paletti minimi previsti dalla normativa, ha deciso di dotarsi il titolare, assume un ruolo nevralgico per la effettiva tutela dei diritti e delle libertà degli interessati. Infatti, se è vero che il titolare gode oggi con il GDPR di un'ampia discrezionalità sulla conformazione materiale del sistema privacy, sempre all'interno dei principi fissati dal Regolamento, è proprio grazie a questa azione del DPO – per la quale ovviamente dovrebbe anche essere dotato degli strumenti idonei da parte del titolare, in particolare per strutture di dimensioni rilevanti – che l'organizzazione potrà adeguarsi e conseguentemente innalzare i propri livelli di *compliance* alla normativa e di tutela dei dati personali. Il DPO, quindi, viene inserito, con tale compito, all'interno di un modello di miglioramento continuo che sostanzialmente ricalca il *ciclo di Deming*[56]. In questa logica il DPO assume, in pratica, il ruolo di una sorta di *auditor interno* all'organizzazione, ma sostanzialmente terzo rispetto a questa. Un modello così impostato dovrebbe presentare il vantaggio di essere proattivo rispetto alle singole problematiche che potrebbero affliggere la tutela dei dati personali nell'organizzazione di riferimento. Tale modello inoltre potrà, ove correttamente attuato, intervenire

[54] A riguardo, va rilevato che, per una corretta interpretazione dello svolgimento dei compiti assegnati al DPO, quest'ultimo (in particolare se "interno") non dovrà cadere nell'errore di sostituirsi al titolare (o al responsabile) del trattamento, né il titolare potrà pensare di delegare il proprio ruolo al DPO. Infatti, ove si verificasse una malaugurata ipotesi del genere, si violerebbe la *ratio* del Regolamento mediante la separazione tra il soggetto che ha il potere di incidere sulla conformazione dell'organizzazione in ottica di tutela della privacy (titolare) e la relativa responsabilità. Ciò creerebbe, inoltre un cortocircuito tra controllore e controllato, nel senso che ove il DPO materialmente dovesse intervenire in via diretta sulla conformazione o su documenti del sistema privacy andando a modificare a suo piacimento la conformazione dello stesso, da una parte va rilevato che in caso di problemi, come già rilevato, comunque risponderebbe il titolare, ma, inoltre, il DPO si troverebbe contemporaneamente nella posizione di controllato e di controllore, cosa ovviamente non consentita dalle norme oltre che evidentemente irrazionale. Così anche nelle consulenze che verranno richieste al DPO questo dovrà fornire al titolare le indicazioni necessarie per poter applicare correttamente la normativa in materia ma non dovrà predisporre materialmente i relativi documenti del sistema privacy. Peraltro va rilevato che, in particolare in organizzazioni di dimensioni elevate, da una parte solo ed esclusivamente il singolo responsabile dell'ufficio o della funzione che si starà esercitando avrà il controllo e la visione completa sulle varie implicazioni che un determinato trattamento di dati personali potrebbe avere sulle variabili che è chiamato a gestire; dall'altra sarebbe materialmente impossibile per un DPO sostituirsi al lavoro di tutti gli addetti che dovessero porre in essere azioni che incidono sul sistema privacy dell'organizzazione. Ma non di meno va tenuto in debito conto che impegnare l'attività del DPO ad un tale livello di dettaglio applicativo materiale delle norme lo assorbirebbe totalmente distogliendolo proprio dalle altre attività sistemiche che solo lui, con la sua elevata professionalità e visione d'insieme, verosimilmente potrebbe svolgere nel supporto al titolare.

[55] Art. 39, c. 1, «b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo».

[56] Il *ciclo di Deming* (o *ciclo di PDCA*, acronimo dall'inglese *Plan – Do – Check – Act*, in italiano "Pianificare - Fare - Verificare - Agire") è un metodo di gestione iterativo in quattro fasi utilizzato per il controllo e il miglioramento continuo dei processi e dei prodotti, spesso alla base dei moderni sistemi di gestione della qualità.

sia prima che si verifichi un problema di non corretta gestione dei dati personali, ma anche di migliorarsi nel tempo, essendo in grado di fare tesoro delle esperienze passate così da produrre un costante innalzamento dei livelli di tutela nella protezione dei dati personali degli interessati.

Il terzo punto dell'art. 39, alla lettera *c)*, prevede che il DPO sia obbligato, ove coinvolto, a fornire il proprio parere[57] nel caso in cui il titolare, valutata la tipologia di trattamento da porre in essere, ritenga sussistente l'obbligo di attivazione di una specifica procedura prevista dal regolamento per valutare in via preventiva la rischiosità di questo (valutazione d'impatto sulla protezione dei dati)[58]. In questo caso l'obbligo, alle condizioni previste dal Regolamento, di condurre la procedura ricade sul titolare in quanto ultimo responsabile dell'organizzazione interna e quindi della corretta implementazione del sistema privacy. L'eventuale coinvolgimento del DPO, tuttavia, serve al titolare per fornire un qualificato parere volto a rilevare eventuali rischi relativi al trattamento dei dati coinvolti, in particolare con riferimento alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento[59]. In caso di attivazione del DPO, infatti, da una parte il titolare si dota della visione di un esperto nella valutazione dei rischi per le libertà ed i diritti fondamentali coinvolti, ma dall'altra non potrà ignorare tale parere senza assumersene la relativa responsabilità soprattutto ove questo fosse palesemente fondato. Infatti, se dall'attivazione di tale trattamento, nonostante il parere contrario del DPO, dovessero derivare eventuali lesioni dei diritti degli interessati, ciò realisticamente potrebbe incidere sulla quantificazione di eventuali sanzioni a discapito del titolare da parte del *Garante per la protezione dei dati personali* (in seguito Garante) in una conseguente eventuale ispezione. Proprio per tale motivo, in più occasioni pubbliche, gli uffici del Garante hanno sottolineato l'importanza della tracciabilità dei pareri emessi dai DPO, che possono così diventare, di fatto, un importante elemento di pressione nei confronti di eventuali titolari che ritenessero di trascurare eventuali rischi per i diritti degli interessati[60].

6. Segue*: d) il rapporto con il Garante: verso una "rete" globale della protezione dei dati personali?*

Gli ultimi due punti dell'art. 39, c. 1, *d)* ed *e)*[61], tra i compiti del DPO dispongono anche che questi debba «cooperare con l'autorità di controllo» (segnatamente, nel nostro ordinamento, con il Garante[62]) e al punto *e)* che debba fungere, ove competente, da *punto di contatto* con questo. In

[57] Art. 39, c. 1, «c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35».

[58] Indicata normalmente con il sintagma inglese *Data Protection Impact Assessment* (DPIA), su cui per approfondimenti v. R. BINNS, *Data protection impact assessments: a meta-regulatory approach*, in *International Data Privacy Law*, 1/2017, Vol. 7, 22-35.

[59] Cfr. Art. 39, «2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo».

[60] In altri istituti il Regolamento, ad es. in caso di presunto *data breach* (cioè in caso di una perdita o indisponibilità di dati personali oggetto di trattamento da parte del titolare), ha previsto l'obbligo di coinvolgimento del DPO e, in caso di *dissenting opinion*, l'annotazione su di un apposito registro dedicato ai *data breach* di cui normalmente è responsabile il titolare. Anche in questa ipotesi la normativa prevede che resterà in capo al titolare l'ultima parola nel decidere se ci si trovi o meno di fronte ad un *data breach* e quindi se attivare la relativa comunicazione al Garante dei dati personali, ma anche in questa ipotesi tale elemento può essere tenuto in considerazione *ex post* nella quantificazione di eventuali sanzioni da comminare al titolare da parte del Garante. Uno dei rischi applicativi a riguardo potrebbe essere rappresentato da una interpretazione del DPO eccessivamente *difensiva* che faccia automaticamente produrre a quest'ultimo sempre e comunque pareri di sussistenza del *databreach* proprio per evitare eventuali rischi di rivalsa contrattuale da parte del titolare che, in ipotesi opposta, avesse evitato di segnalare al Garante un *data breach* su parere errato del DPO.

[61] Art. 39, 1, «d) cooperare con l'autorità di controllo; e

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione».

[62] Nello studio di tale autorità indipendente si dovrà tenere in debito conto il fatto che questa, a differenza di altre (es. *Autorità garante per la concorrenza ed il mercato* – AGCM o *Antitrust*, *Autorità per le garanzie nelle comunicazioni* – AGCOM), è portatrice della tutela di un diritto fondamentale e non di un settore.

particolare viene esplicitamente richiamato il caso in cui vi fosse la necessità di attuare una *consultazione preventiva* del Garante[63] ai sensi dell'art. 36 del GDPR, ma si prevede inoltre, secondo il modello della c.d. "norma in bianco", che il DPO, a sua discrezione, possa consultare gli uffici del Garante su qualsiasi altra questione, attinente alle sue competenze ed ove lo ritenesse opportuno.

Con quest'ultima previsione, quindi, il Garante si configura come una sorta di *consulente di ultima istanza* nei confronti dei DPO e quindi dei titolari. A riguardo si badi che la norma non riporta alcun preventivo assenso o potere ostativo in capo al titolare, ne consegue che tale potere *consultivo*, ma che a ben vedere può anche assumere un ruolo "materialmente *informativo"* a disposizione del DPO nei confronti del Garante[64], rappresenta un rilevante istituto formalizzato di interazione tra i due soggetti. Questo, infatti, può costituire già un primo ma importante tassello nella creazione di un rapporto a "rete" che sempre più si inizia a formalizzare tra Garante, garanti e singoli DPO (peraltro non solo dei Paesi membri) nella sorveglianza sull'applicazione delle norme in materia di tutela dei dati personali. Così con la positivizzazione, fra i compiti minimi obbligatori del DPO, anche di quello di cooperazione con il Garante, il legislatore europeo ha creato le condizioni formali e materiali per un rapporto diretto tra le "braccia armate" della tutela della privacy (cioè le Agenzie nazionali, che rappresentano i soggetti pubblici in prima linea nel controllo sull'*enforcement* della normativa in materia e che dispongono di rilevanti poteri ispettivi e sanzionatori) ed i DPO. Cioè proprio con quegli interlocutori privilegiati che, all'interno delle organizzazioni, grazie alle caratteristiche di elevata professionalità e competenza in materia di tutela dei dati personali che li dovrebbero contraddistinguere, sono in grado di parlare la medesima lingua del Garante e quindi ben si possono fare portatori, quali soggetti terzi indipendenti rispetto ai titolari che li hanno designati, delle istanze relative all'organizzazione nella quale operano e che quindi ben conoscono, sia *rispetto*, che *da parte*, del Garante[65].

Il rapporto tra questi soggetti viene quindi a conformarsi in modo biunivoco, dal momento che il DPO diventa, a determinate condizioni, abilitato a rapportarsi con il Garante, dall'altro anche il Garante, ove abbia bisogno di informazioni, sempre in relazione alle proprie competenze, su questioni che coinvolgono l'organizzazione nella quale è designato il DPO, si potrà rivolgere a questo quale «punto di contatto» per avere prime informazioni utili[66]. Ovviamente il DPO in questa azione non si

---

[63] Cioè nel caso in cui la valutazione d'impatto relativa ad un trattamento prevista dall'art. 35 del Regolamento, presentasse un rischio elevato per i diritti e le libertà fondamentali degli interessati, in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

[64] Inizia così a fare capolino, nell'attuale scenario normativo, la questione della natura del rapporto tra DPO e Garante. E cioè se il DPO a determinate condizioni, si pensi ad esempio se a seguito di ripetute violazioni del Regolamento da parte del titolare, in particolare ove tali violazioni pongano a serio rischio i diritti e le libertà fondamentali degli interessati, sia soggetto ad un vero e proprio obbligo di segnalazione nei confronti del Garante (oltre quello già previsto nei confronti del titolare). Così non si può escludere che tale istituto possa essere utilizzato, in modo alternativo, per segnalare in via indiretta, con il pretesto della consultazione preventiva facoltativa, eventuali situazioni di disapplicazione del Regolamento da parte di titolari restii ad applicare la normativa in materia e presso i quali il DPO opera. Va rilevato, infatti, che ad oggi non sembra possa sussistere un vero e proprio obbligo di riferire, da parte del DPO, al Garante o all'Autorità giudiziaria (non rivestendo il DPO la qualifica di pubblico ufficiale alle dipendenze del Garante o di ufficiale di polizia giudiziaria), anche se tale strumento potrebbe rappresentare una sorta di invito indiretto al Garante ad accendere un riflettore sull'organizzazione dalla quale proviene la segnalazione da parte del DPO sulla questione posta. Certo la tematica resta ancora da indagare con un maggior livello di approfondimento, con particolare riguardo anche agli aspetti giuslavoristici collegati al rapporto che si viene ad instaurare tra titolare e DPO, in particolare con riferimento agli obblighi di riservatezza a questo connessi e alle eventuali differenze relative alla designazione di un DPO "interno" o "esterno" all'organizzazione.

[65] Avere un interlocutore privilegiato e competente all'interno delle organizzazioni che trattano dati personali e che, avendo l'obbligo di un DPO, sono proprio quelle che presentano un maggior livello di rischiosità per i diritti e le libertà fondamentali degli interessati, può risultare elemento strategico proprio nei tempi di risposta ad eventuali minacce per la tutela dei dati personali, sia in ottica reattiva che proattiva. Ancora una volta si pensi alle procedure e tempistiche di gestione e risposta previste in caso di *data breach* in cui son previsti i termini massimi di segnalazione espressi in termini di ore (72!).

[66] Ad esempio si pensi al caso in cui, a seguito di notifica al Garante di *data breach*, quest'ultimo avesse bisogno di ulteriori informazioni sullo stesso. In questo caso potrebbe contattare il DPO, che però si dovrà limitare a fare da interlocutore privilegiato nei confronti del Garante, ma mai da "avvocato" del titolare. Infatti il DPO è, in base alla

potrà sostituire in alcun caso al titolare rispondendo al Garante al suo posto o redigendo la documentazione per la consultazione preventiva, così come «tutte le informazioni relative ai trattamenti dati e ai relativi rischi associati dovranno essere necessariamente forniti dal titolare o dal responsabile»[67].

Passando ad osservare il rapporto tra i DPO ed i Garanti nazionali, alla luce del Regolamento e nell'ottica di indagine qui assunta che coinvolga anche gli aspetti di "diritto vivente", questo assume nuove sfumature di estremo interesse e degne d'indagine. Infatti se, limitandosi a quanto previsto dalla struttura formale configurata dal Regolamento, si potrebbe ipotizzare un mero rapporto tra un soggetto pubblico (le singole autorità tecniche indipendenti nazionali – cioè i Garanti), ed un soggetto sostanzialmente di tipo privatistico (i singoli DPO designati, con alcune differenze, peraltro significative se si ragiona su DPO *interni*, e quindi già dipendenti dell'organizzazione, o *esterni*), approfondendo l'attuale evoluzione materiale di tale rapporto la conformazione sembra iniziare ad assumere toni meno netti, in particolare con riguardo alla figura del DPO. Se poi tale rapporto viene indagato anche alla luce del contesto applicativo che sta assumendo la normativa in materia di tutela dei dati personali, le differenze tra la strutturazione teorica del modello regolativo e la relativa risultante applicativa sembrerebbero iniziare a divaricarsi ulteriormente. Il rapporto formalizzato dal Regolamento, quindi, può essere letto in senso evolutivo, oltre che alla luce dei primi aspetti accennati sopra, anche, ad esempio, osservando alcune significative iniziative dedicate esclusivamente ai DPO[68], operanti presso soggetti pubblici, e promosse da singoli garanti nazionali. Tali iniziative sono state lodevolmente volte sia a migliorare i livelli di uniformità applicativa del Regolamento, attraverso la condivisione con i DPO coinvolti della visione applicativa minima di questo; sia alla creazione di un rapporto privilegiato tra Garante e singoli DPO (in questo caso del settore pubblico, con tutte le sue peculiarità), sempre e comunque nel pieno rispetto dei rispettivi ruoli[69].

---

normativa, di fatto prevalentemente portatore delle istanze degli interessati all'interno dell'organizzazione, il titolare, invece, degli interessi dell'organizzazione. Così in caso contrario si verrebbe a creare un palese conflitto di interessi tra i ruoli e le funzioni dei due soggetti in materia. Ovviamente nulla vieta al Garante di contattare direttamente il titolare, ove lo ritenesse necessario. La scelta di sentire preliminarmente il DPO sarebbe dettata semplicemente da esigenze di efficienza comunicativa e di prima rappresentazione della situazione da parte di un soggetto terzo indipendente rispetto all'organizzazione, che si presume possa avere una maggiore lucidità, nel rappresentare l'accaduto e nel fornire ulteriori elementi sullo stesso, oltre che, molto probabilmente, una maggiore conoscenza tecnica del sistema privacy coinvolto rispetto anche forse allo stesso titolare che dovrà occuparsi di tutti gli aspetti gestionali dell'organizzazione, compreso quello della privacy.

[67] G.M. RICCIO, *Art. 39*, in G.M. RICCIO, G. SCORZA, E. BELISARIO (curr.), *GDPR e normativa privacy*, cit., 352.

[68] Si pensi ad esempio anche alle *faq* del Garante o alle precisazioni del WP-29, oggi sostituito dal Comitato europeo per la protezione dei dati, su cui ad esempio cfr., A. D'AGOSTINO, E. MAGAGNOLI, *Regolamento UE 2016/679 – Il Data Protection Officer alla luce dei recenti chiarimenti del WP-29 e dell'Autorità garante per la protezione dei dati personali*, in *Ilsole24ore*, 23 gennaio 2018, 1-3.

[69] A titolo di esempio si pensi al progetto *T4data* promosso dal garante italiano che ha previsto una serie di iniziative e di incontri di formazione specificamente destinati ai DPO delle pubbliche amministrazioni (materiali e descrizione completa reperibili in www.garanteprivacy.it/ regolamentoue/ formazione/ t4data). Grazie a questo si è di fatto resa possibile la condivisione con i DPO della lettura interpretativa fatta dal Garante del Regolamento, ma anche dello stesso ruolo del DPO. Tali seminari sono poi stati anche messi a disposizione *on line* per i DPO che non sono potuti intervenire ai singoli incontri, che va segnalato hanno registrato la piena affluenza, a testimonianza anche della domanda di un minimo di certezze interpretative sulla normativa, in particolare in fase di prima applicazione. Altro elemento degno di nota, sempre all'interno dello stesso progetto, è rappresentato dalla promozione, con la collaborazione di altre autorità europee, anche della redazione di un manuale tipo del DPO (redatto originariamente in lingua inglese e successivamente tradotto in italiano) con il quale sono stati forniti ai DPO varie attività ed esempi di come il DPO dovrebbe materialmente interpretare il proprio ruolo e svolgere le funzioni a questo assegnate. Ora, benché il manuale sia stato corredato di ampio *disclaimer* in premessa che sottolinea l'assenza di qualsiasi valenza ufficiale e vincolante dello stesso, e che questo rappresenti esclusivamente un esempio di buona pratica, ben si comprenderà che, in assenza di ulteriori riferimenti ufficiali e alla luce del fatto che tale documento è nato sotto gli auspici di più di una autorità garante nazionale, comunque il contenuto dello stesso possa ben rappresentare uno strumento per indirizzare verso la conformazione operativa rappresentata l'esercizio materiale delle funzioni dei DPO nelle rispettive organizzazioni. Con questo esempio di possibile buona pratica, che sicuramente può essere letto come strumento realizzato nel supporto ed in ottica di servizio ai DPO che operano presso soggetti pubblici, vengono quindi introdotti in ottica materiale prassi e interpretazioni della normativa difficilmente derogabili dai singoli DPO, salvo essere disposti ad assumersi l'onere di dimostrare nelle varie sedi la bontà

Così andrà verificato se e in che misura in un prossimo futuro, con una maggiore stabilizzazione materiale del ruolo dei DPO nei vari ambiti operativi, ci si stia avviando o meno verso un processo che possa portare le Autorità nazionali a declinare in modo più o meno rilevante le previsioni formali previste dal Regolamento in relazione al ruolo materialmente svolto dai DPO[70]. Tale processo, infatti, potrebbe far convergere sempre più la realtà applicativa delle tutele in materia di dati personali verso un modello materiale europeo il cui rapporto con i singoli Garanti si caratterizzi per una strettissima relazione bidirezionale che trasformi i DPO, ove presenti, in una sorta di "estensioni operative" di questi all'interno proprio di quelle organizzazioni che maggiormente possono incidere sulla lesione di quei diritti e di quelle libertà fondamentali che il Regolamento in via diretta ed indiretta si prefigge di tutelare.

Per completare il quadro qui necessariamente solo tratteggiato, infine e passando ad una prospettiva di osservazione multilivello, può risultare interessante almeno accennare, da una parte, al rapporto di cooperazione previsto dallo stesso Regolamento[71] tra i garanti europei e all'istituzionalizzazione del Comitato europeo per la protezione dei dati; dall'altra, anche a quello, ormai formalizzato, tra i singoli garanti statali (ove presenti) a livello internazionale[72]. Infatti tali rapporti producono e produrranno necessariamente ripercussioni sulla conformazione giuridica del ruolo materiale che dovranno svolgere i DPO, a causa della influenza delle posizioni condivise dai garanti a livello internazionale e veicolate da ognuno di questi nei rispettivi ordinamenti nazionali, negli spazi di discrezionalità concessi dalle rispettive normative alle quali sono sottoposti. Maggiore sarà il livello di condivisione di tali posizioni e più velocemente queste entreranno, anche grazie ai DPO, nelle differenti organizzazioni. Da tale prospettiva d'indagine, quindi, sembrerebbe sempre più netta la direzione presa dal modello: una sorta di conformazione "a rete" della sorveglianza sull'applicazione e sull'*enforcement* del modello europeo di protezione dei dati personali, che coinvolge soggetti pubblici e a rilevanza pubblica (DPO) con sempre maggiori correlazioni reciproche, anche oltre i confini dell'Unione.

Nella dimensione europea, così, si iniziano già a rilevare maggiori elementi di circolazione dei modelli applicativi condivisi dai Garanti europei contenenti principi, standard e strumenti volti alla tutela dei dati personali. Si assiste, inoltre, anche ad un ulteriore fenomeno, e cioè all'affermarsi, nella prassi ed in assenza di riferimenti certi interni, di alcuni provvedimenti emanati da Autorità di altri

---

delle proprie interpretazioni della normativa. Così potrebbe anche capitare che con tali modalità vengano materialmente veicolate sul DPO funzioni ulteriori rispetto a quelle minime esplicitamente previste dal Regolamento o contrattualizzate spingendosi anche al limite della discrezionalità prevista dalle norme. A titolo di esempio riguardo a quest'ultimo punto, si pensi alla funzione apparentemente esclusiva assegnata ai DPO nel rispondere alle istanze degli interessati che sembrerebbe emergere dal citato manuale/modello, ma che non sembra affatto rispondere a quanto previsto dalla normativa, che non vieta né agli interessati di rivolgersi direttamente al titolare né che quest'ultimo possa rispondere direttamente a questi.

[70] A riguardo va anche rilevato che, ove le Autorità dovessero esagerare nell'interpretazione estensiva del ruolo dei DPO, potrebbero ben intervenire le Corti, ed in particolare quella di Giustizia, o direttamente il legislatore europeo dettagliando i limiti interpretativi delle relative norme e ristabilendo confini più netti alla conformazione regolativa della materia.

[71] Cfr. Capo VII «Cooperazione e coerenza», artt. 60-76 del Regolamento.

[72] Si pensi ai costanti appuntamenti, che si svolgono ormai dal lontano 1979, rappresentati dalle *Conferenze mondiali dei Garanti privacy* (ICDPPC), giunti alla quarantaduesima edizione, che si terrà quest'anno in Messico.

Proprio nel corso dell'ultima conferenza dal titolo «*Convergence and connectivity raising global data protection standards in the digital age*», tenutasi a Tirana dal 21 al 24 ottobre 2019 e alla quale hanno partecipato oltre 120 Autorità per la protezione dei dati, si è deciso di istituire la *Global Privacy Assembly* (GPA) creando di fatto un nuovo protagonista tra le *istituzioni globali* in materia di tutela dei dati personali. Sempre nel corso dell'ultima Conferenza vi è stata l'approvazione di ben sei risoluzioni. Tra le linee strategiche in queste adottate si può segnalare: il riconoscimento della privacy come diritto fondamentale per il buon funzionamento delle democrazie; il contrasto sui social media ai messaggi inneggianti al terrorismo; una più intensa cooperazione tra le Autorità che tutelano i dati personali e quelle che operano a tutela dei consumatori e della concorrenza; la riduzione dell'errore umano nelle violazioni dei dati. Proprio sul primo tema, e cioè sulla «Risoluzione sulla privacy come diritto umano fondamentale e prerequisito per l'esercizio di altri diritti fondamentali», si è speso il Garante italiano come co-sponsor. Le linee guida complete sono reperibili sul sito del Garante al seguente link *www.garanteprivacy.it/ home/ docweb/ -/ docweb-display/ docweb/ 9197083#3*.

Stati membri a seguito delle scelte applicative dominanti effettuate dagli stessi DPO nello spazio eurounitario. Proprio grazie alla circolazione e alla formalizzazione di momenti di confronto nell'applicazione delle differenti normative in materia di tutela dei dati personali, non si può escludere che gli istituti più efficaci ed efficienti possano trovare fortuna anche a livello internazionale, entrando a far parte nel tempo di quel nocciolo duro che costituirà l'essenza della *costituzione materiale globale*[73] della tutela dei dati personali. Così, ove questa influenza reciproca trovasse sempre maggiori riscontri, la figura del DPO verrebbe ad assumere un nuovo livello di rilevanza pubblica, addirittura di rango europeo, meritevole di ulteriori livelli di indagine.

7. *Per non concludere*

Data l'economia del presente lavoro, diventa qui impossibile sviluppare compiutamente le suggestioni sopra appena tratteggiate. Sia sufficiente rilevare che l'indagine di tali complesse tematiche, anche attraverso le quali passa la conformazione materiale del modello costituzionale europeo di tutela dei dati personali, può contribuire a far meglio comprendere i meccanismi istituzionali che stanno portando, a velocità sempre maggiore, verso l'approdo ad una costituzionalizzazione materiale globale del diritto alla tutela dei dati personali e quindi della privacy, almeno con riferimento agli elementi essenziali. Peraltro, tale processo, di fatto, si sta già scrivendo quotidianamente con le scelte fatte dai legislatori[74], dalle Corti, dai garanti, ma come visto, in parte, anche dagli stessi DPO nel rapporto con i singoli titolari ed i garanti stessi. La fissazione del livello materiale minimo europeo e mondiale di tutela dei dati personali si giocherà, quindi, in una logica di cinico darwinismo normativo globale figlio della razionalità delle regole che verranno poste a fondamento della normativa in materia di tutela dei dati personali, e di quanto queste siano compatibili con i meccanismi di produzione della ricchezza nel mondo globalizzato e quindi, ad oggi, di sopravvivenza stessa del genere umano[75].

Resta però aperto, tra gli altri, il problema dei problemi: chi inciderà, ed in quale misura, sulla conformazione di queste regole? Gli Stati? Le super potenze economiche con o senza l'UE? I garanti, organizzati con un modello "a rete" multilivello? O le scriveranno le multinazionali, sempre più spesso monopoliste delle tecnologie strategiche e le cui scelte diventano, di fatto, oggi più di ieri difficilmente contrastabili sul mercato digitale globale dai singoli ordinamenti statali?

---

[73] Su cui un interessante primo studio del 2013, cfr. K.A. BAMBERGER, D.K. MULLIGAN, *Privacy in Europe: Initial Data on Governance Choices and Corporate Practices,* in T*he George Washington Law Review*, 81/2013, Vol. 81, 1529-1664.

[74] Si pensi agli effetti che produrrà l'approvazione del c.d. Regolamento *e-Privacy* che sostituirà l'attuale Direttiva *e-Privacy* (Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al «trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche») e completerà alcuni importanti aspetti del GDPR. Se e quando avverrà visto che, nonostante il lungo iter legislativo che si protrae ormai da anni, non si riesce ad arrivare ad un accordo sui contenuti ed il COREPER, a novembre 2019, ha bocciato la relativa bozza che gli era stata sottoposta.

[75] Su cui cfr. Antonello Soro, Presidente dell'Autorità Garante, il quale rileva che «Il passo che resta da fare, raccogliendo una delle sfide più importanti che il legame tra tecnologia, nuovi diritti e prevenzione pone alle nostre generazioni, è quello del riconoscimento universale del diritto alla protezione dei dati personali, quale primo presupposto di libertà del XXI secolo.

È una bella sfida per le democrazie di tutto il mondo», A. SORO, *Persone in rete. I dati tra poteri e diritti*, Roma, Fazi, 2018, 135, richiamato anche in C. TITO, *Perché la democrazia oggi è fondata sulla nostra privacy*, cit.., 2. Sui meccanismi di circolazione e di selezione dei modelli regolativi a livello globale cfr. G. DI PLINIO, *Il common core della deregulation*, Milano, Giuffrè, 2005.