CAPITOLO 1

La figura del DPO nel regolamento europeo n. 2016/679

di Gian Marco Pellos

Sommario: 1. Il GDPR: contesto, principi e prospettive. – 2. Il DPO: i riferimenti normativi e i documenti delle istituzioni. – 3. Chi deve dotarsi di un DPO? – 4. Cosa si intende per "trattamento dati su larga scala"? – 5. Competenze e caratteristiche del DPO. – 6. La nomina del DPO. – 7. La posizione del DPO all'interno della struttura. – 8. L'analisi del rischio. – 9. La *Data Protection Impact Assestment*. – 10. Il decreto legislativo n. 101 del 10 Agosto 2018: le modifiche di rilevo per il DPO.

1. Il GDPR: contesto, principi e prospettive

La data del 25 maggio 2018 ha segnato indubbiamente uno spartiacque fondamentale in tema di tutela dei dati personali.

L'entrata in vigore del Regolamento europeo n. 679/2016, denominato anche *General Data Protection Regulation* (Regolamento Generale per la Protezione dei Dati), infatti, ha imposto a cittadini, imprese e professionisti di tutti i paesi membri dell'Unione Europea la necessità di aggiornare e rendere più efficienti le misure di protezione dei dati personali.

Delle molte riforme che ogni anno vengono varate sulla base del diritto europeo, il GDPR non è di quelle che possono essere lasciate alla sola attenzione di ristrette cerchie di addetti di lavori.

Basti solo considerare alcuni fattori:

Il primo è che l'odierna economia, fondata sulle tecnologie digitali, si muove e si sviluppa proprio sulla condivisione di dati e informazioni personali, utilizzati per creare ed implementare servizi modellati *ad hoc* sulle esigenze degli utenti che ne usufruiscono, ed è ovvio che per fare questo è necessario l'utilizzo continuo di dati personali.

Il secondo fattore, collegato al primo, è che non è dato rinvenire alcun settore professionale che non sia coinvolto nella necessità di conservare, trattare e pertanto tutelare dati.

Non vi è nessuno quindi che possa considerare come secondario l'adeguamento normativo su questo aspetto.

Inoltre, vale la pena sottolineare che si è di fronte a uno dei primi casi in cui un diritto fondamentale della persona viene disciplinato direttamente dall'Unione Europea per mezzo di un Regolamento e non con una direttiva da lasciar recepire ai diversi stati membri.

Una decisione "invasiva" nei confronti degli ordinamenti interni dei vari stati membri ma che si spiega proprio con la necessità di uniformare la regolamentazione di una materia che evidentemente viene considerata strategica.

D'altro canto, nell'odierno mondo globalizzato, solo una legislazione univocamente riconosciuta e applicata in tutto il continente può fronteggiare le sfide globali poste dai grandi paesi e dai colossi dell'industria digitale[1].

D'altro canto, si assiste ormai quasi quotidianamente al moltiplicarsi di notizie riguardanti violazioni di dati: si pensi ai famosi episodi del *Datagate* o al recente scandalo *Cambridge Analytica*, passando per numerose altre vicende meno note ma non meno significative, che riguardano tanto le grandi aziende multinazionali quanto piccoli imprenditori, professionisti e semplici cittadini.

Non stupisce allora constatare come la normativa previgente[2], concepita a metà degli anni '90, si sia rivelata nel tempo insufficiente per fare fronte alle sfide e alle problematiche che caratterizzano l'odierno contesto in materia di privacy.

La delicatezza dell'argomento e la molteplicità degli interessi in gioco hanno fatto sì che la gestazione di una nuova normativa, comune a tutti gli Stati membri dell'Unione Europea, si sia rivelata lunga e complessa.

Infatti, l'idea di dare vita a tale normativa prese corpo già nel 2012 con la *Proposta di Regolamento del Parlamento Europeo e del consiglio*

---

[1] Per approfondimenti: L. Califano, C. Colapietro (a cura di), *Innovazione tecnologica e valore della persona, Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Università degli Studi di Roma Tre, collana CRISPEL, Editoriale Scientifica, 2017.

[2] Trattasi della "Direttiva n. 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati", recepita in Italia con il famoso d.lgs. 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali".

concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati del 25 gennaio 2012[3].

Da allora 4 anni ci sono voluti per vedere l'approvazione definitiva del cosiddetto *"Pacchetto di protezione dati"* comprendente:

- **Regolamento (Ue) 2016/679 Del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)** nominato in via breve, come detto, GDPR o RGPD, a seconda che si preferisca la definizione in lingua inglese o italiana.
- **Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.**

Il GDPR è stato quindi approvato il 27 aprile 2016; è formato una serie di *Considerando* introduttivi e da 11 Capi per un totale di 99 Articoli.

Rispetto alla precedente legislazione si fa portatore di nuovi e penetranti principi, a volte mutuati dalla giurisprudenza della Corte di Giustizia dell'Unione Europea e dei singoli stati membri, a volte introducendo elementi di fatto nuovi con i quali gli operatori devono confrontarsi.

Per questi motivi, prima di analizzare a fondo la figura che ci interessa in questa sede, ossia il *Data Protection Officer* (in italiano *Responsabile della protezione dei dati*), sarà opportuno prendere consapevolezza dei più importanti contenuti nel *General Data Protection Regulation.*

The Right to Data Portability (Diritto alla portabilità dei dati)

Il diritto alla portabilità dei dati è espresso in particolare all'art. 20 del GDPR e prevede che, ricorrendo specifici presupposti[4], i dati di un sog-

[3] L'*iter legis* del provvedimento è consultabile sul sito "www.eurlex.eu" (https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:52012PC0011)

[4] I presupposti, delineati all'art. 20, par. I, Reg. (UE) n. 2016/679 prevedono il: "a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e b) il trattamento sia effettuato con mezzi automatizzati".

getto debbano poter essere trasferiti in un formato "*strutturato, di uso comune e leggibile da dispositivo automatico"*[5].

Tale previsione è pienamente comprensibile perché, in una società dove è fondamentale il ruolo delle comunicazioni digitali, trasferire informazioni da un supporto ad un altro o da una struttura ad un'altra è indispensabile per garantire realmente un controllo sui propri dati, senza del quale è del tutto superfluo parlare di diritto alla *privacy* e di tutela di quelle persone cui quei dati si riferiscono.

Right to erasure ('right to be forgotten') – Diritto all'Oblio

Con tale nome si indica il diritto enunciato nell'art. 17 del GDPR

Fra tutte le novità introdotte dal Regolamento, il diritto alla cancellazione dei dati è forse quella più nota, trattandosi di un argomento che spesso balza agli onori delle cronache a causa dell'eterno conflitto con il diritto di cronaca e di informazione.

Di fatto, il diritto all'oblio si sostanzia nella possibilità, in capo al soggetto interessato, di ottenere la cancellazione di dati personali che lo riguardano ogniqualvolta non vi sia più un pubblico interesse alla pubblicazione degli stessi o non vi sia più il presupposto giuridico su cui si fondavano la raccolta, il trattamento e la diffusione.

Non si tratta, quindi, di una prerogativa riconosciuta soltanto a personaggi pubblici o soggetti che possono comunque essere rimasti coinvolti in vicende di grande clamore mediatico.

Invero ciascuno, nel momento in cui intenda revocare il suo consenso ad un determinato trattamento o decida di cancellare l'iscrizione a un certo servizio, ha diritto a vedere cancellati i dati inerenti alla propria persona, detenuti dal titolare di quel trattamento.

Privacy by design e privacy by default (Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita)

I concetti di *privacy by design* e *privacy by default* erano già entrati negli ultimi anni nel panorama giuridico di questa materia; in particolare nel corso della trentaduesima *International Conference of Data Protection and Privacy Commissioners* era stata sottolineata la necessità di riconoscere la *privacy by design* come componente essenziale nel quadro della protezione dei dati personali e l'opportunità di adottare, conseguentemen-

[5] Art. 20, par. I, Regolamento (UE) n. 2016/679.

te, principi in materia che permettessero di configurare la protezione della privacy come modalità predefinita[6]

Tali principi vengono ora enucleati nel Regolamento Europeo all'articolo 25.

Con l'espressione *privacy by design*, ci si riferisce alla necessità di tutelare i dati sin dal momento in cui un sistema viene progettato, avendo cura di analizzare sin da principio i possibili rischi, prevedendo quindi il loro manifestarsi.

Con l'espressione *privacy by default* si indica invece il dovere di fornire, come impostazione predefinita, la massima tutela possibile ai dati personali che vengono immessi all'interno di un sistema in modo che essi siano trattati in conformità a quanto previsto dalla normativa sulla privacy.

Si tratta, come è evidente, di due facce della stessa medaglia, giacchè entrambe le definizioni rimandano alla necessità, quando si proceda alla ideazione e progettazione di un sistema che preveda l'utilizzo di dati personali, di prevedere la protezione della privacy e il rispetto della normativa in materia *ab orgine*.

Non stupisce che si sia resa necessaria questa forma rafforzata di tutela visto che le innovazioni tecnologiche e tecniche hanno fatto sì che l'utilizzo di dati personali sia una costante pressoché generale e irrinunciabile, cui deve corrispondere la crescita di una cultura diffusa della privacy, cui queste disposizioni tendono, affinchè questo diritto non sia considerato più come mero adempimento formale bensì quale aspetto fondamentale e *conditio sine qua non* per l'ideazione e realizzazione di nuovi sistemi e servizi.

Accountability (Responsabilità del titolare del trattamento)

L'accountability è un vero e proprio pilastro del nuovo Regolamento Europeo, lo permea integralmente e viene ivi descritto principalmente all'art. 24.

In buona sostanza, questo principio prevede che il titolare del trattamento debba mettere in atto, aggiornandole periodicamente, misure tecniche ed organizzative che siano adeguate a garantire la sicurezza dei dati trattati e la conformità alla normativa vigente.

---

[6] *Cfr.* 32nd International Conference of Data Protection and Privacy Commissioners, *Resolution on Privacy by Design* Jerusalem, Israel 27-29 October, 2010, disponibile al seguente URL: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf

Si tratta di un approccio *case by case*, non più determinabile a priori perchè necessita del concreto affronto delle problematiche che vengono in rilievo nei singoli trattamenti.

Questo da un lato rende dinamica la tutela dei dati, cosa indispensabile in un contesto in continuo mutamento come è quello odierno ma dall'altro lato pone sicuramente gli addetti ai lavori in una situazione di incertezza, poiché non ci si può affidare all'ormai superato concetto di "misure minime di sicurezza" presente nel Codice della Privacy, nè ad altri adempimenti meramente formali, per avere la garanzia della propria conformità ai dettami legislativi in materia di privacy.

In base al GDPR, infatti, è doveroso aggiornarsi continuamente ed essere in grado di dare conto della bontà delle scelte fatte per garantire la sicurezza e il corretto trattamento dei dati.

Invero, l'incertezza che consegue alla presa d'atto che non è più sufficiente adempiere a precise prescrizioni normative non è di certo un effetto collaterale ma una chiara finalità della nuova normativa, poiché costrinnge ad un rinnovato approccio al tema della privacy, nel quale vengono valorizzate molto più che in passato la formazione, i connotati professionali, le capacità organizzative e di iniziativa di tutte le figure, *in primis* del *Data Protection Officer*, che trattano i dati all'interno delle aziende, delle pubbliche amministrazioni e delle altre strutture cui il Regolamento si applica.

In altre parole, se fino a poco tempo fa poteva dirsi sufficiente adeguarsi a determinate indicazioni legislative, quali potevano essere quelle contenute nell'allegato B del d.lgs. 196/2003, ora ciò non è più sufficiente e d'altronde sarebbe decisamente inadeguato di fronte all'attuale situazione in cui deve operare un professionista della privacy.

È quindi fondamentale implementare la capacità di analizzare caso per caso e circostanza per circostanza i rischi delle specifiche situazioni in cui ci si può imbattere nel trattamento dei dati e organizzare gli opportuni rimedi sia in fase di prevenzione che al momento del manifestarsi del rischio.

Quello davanti al quale ci si trova è un profondo cambiamento di mentalità che, beninteso, non sarà semplice recepire, soprattutto in un ordinamento giuridico come quello italiano, particolarmente legato a un'impostazione formalistica che difficilmente si adatta alla fluidità e alla duttilità dei principi che sono posti alla base del GDPR ma che, lo si ribadisce, è fondamentale per adeguarsi alle problematiche giuridiche che comporta la tutela dei dati nella società dell'informazione.

2. Il DPO: i riferimenti normativi e i documenti delle istituzioni

Nell'analizzare i contenuti del nuovo Regolamento (UE) n. 2016/679, una delle novità più rilevanti che emergono, soprattutto se raffrontata alla previgente disciplina, riguarda la figura del *Data Protection Officer*, resa in italiano come *Responsabile della Protezione dei Dati – RPD*).

Si precisa sin d'ora che nel corso del manuale, si utilizzeranno entrambe le formulazioni, anche se si ritiene sia più utile l'utilizzo della formula in lingua inglese, dal momento che è così che viene identificata a livello internazionale.

Si tratta, in ogni caso, di una figura che non era presente nel precedente apparato normativo e le cui caratteristiche vengono ora descritte alla sezione IV del Regolamento, agli Artt. 37, 38, e 39.

Sulla base di tali disposizioni normative, si apprende che un DPO deve essere nominato in tutte le pubbliche amministrazioni, con l'eccezione dell'autorità giurisdizionale[7], nonché in tutti i casi in cui i trattamenti richiedano il monitoraggio regolare e sistematico degli interessati su larga scala o nelle ipotesi in cui vengano trattate le particolari categorie di dati ex articolo 9 e 10.

Particolari garanzie circondano questo soggetto.

Oltre a veder riconosciuta la propria indipendenza, infatti, il Data Protection Officer ha diritto ad essere coinvolto nella gestione di tutte le problematiche inerenti alla privacy e a poter usufruire di risorse adeguate per realizzare i compiti che il Regolamento gli affida, che possono essere così sintetizzati:

- Fornire consulenza al titolare o al responsabile in merito agli obblighi normativi;
- Sorvegliare sull'effettiva applicazione del Regolamento all'interno della struttura in cui opera;
- All'occorrenza, esprimersi in merito alla valutazione di impatto sulla protezione dei dati;
- Interfacciarsi con l'autorità di controllo[8];

Si tratta di una figura che si integra con le altre già previste già dalla pregressa normativa, ossia il Titolare del trattamento e il Responsabile del

---

[7] Come si avrà modo di osservare più avanti, il recente decreto legislativo del 10 agosto 2018 n. 101 è intervenuto sul punto stabilendo che anche per le autorità giudiziarie sono tenute alla nomina di un DPO.

[8] *Cfr.* Art. 39, par. 1, *Reg.* (*UE*) n. 2016/*679.*

trattamento, con la doverosa precisazione che, in base a quanto si evince dal testo del Regolamento, non si tratta di una figura dotata di poteri di gestione e intervento diretto sul trattamento, che rimangono in capo al Titolare o, eventualmente, al Responsabile.

Ciò non deve in alcun modo indurre a sottovalutare il ruolo e le responsabilità del DPO, che nelle intenzioni del legislatore europeo si pone come un soggetto quasi *super partes* rispetto agli altri attori presenti in azienda o nella struttura pubblica, proprio in virtù alle prerogative che il Regolamento intende assicurargli e delle caratteristiche che a tal fine richiede.

Il suo ruolo si traduce in una sorta di controllore interno, chiamato a valorizzare e dare attuazione a quel principio di *accountability* cui si è fatto poc'anzi riferimento e che è così importante nella gestione della privacy alla luce della nuova normativa.

Come per ogni novità legislativa, non tutti i dubbi sono sopiti in relazione a quali siano effettivamente i confini di azione e le caratteristiche della nuova figura.

Sotto questo profilo, un aiuto fondamentale in viene dal raffronto con il Considerando 97, che parla di un soggetto che deve avere una conoscenza specialistica ed essere in grado di affiancare l'attività del titolare del trattamento, riuscendo in tal modo a sorvegliare il corretto svolgimento delle procedure inerenti alla privacy nella struttura in cui opera[9].

Le indicazioni fornite dal testo del Regolamento, tuttavia, non si sono

[9] Vale la pena riportare il testo del Cons. 97, Reg. (UE) n. 2016/679: "Per i trattamenti effettuati da un'autorità pubblica, eccettuate le autorità giurisdizionali o autorità giudiziarie indipendenti quando esercitano le loro funzioni giurisdizionali, o per i trattamenti effettuati nel settore privato da un titolare del trattamento le cui attività principali consistono in trattamenti che richiedono un monitoraggio regolare e sistematico degli interessati su larga scala, o ove le attività principali del titolare del trattamento o del responsabile del trattamento consistano nel trattamento su larga scala di categorie particolari di dati personali e di dati relativi alle condanne penali e ai reati, il titolare del trattamento o il responsabile del trattamento dovrebbe essere assistito da una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del presente Regolamento. Nel settore privato le attività principali del titolare del trattamento riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria. Il livello necessario di conoscenza specialistica dovrebbe essere determinato in particolare in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento. Tali responsabili della protezione dei dati, dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente".

rivelate sufficienti a dissipare i dubbi relativi ad una compiuta definizione del DPO e quindi, vista anche la grande attesa che si è venuta a creare sin da subito intorno a questa figura, il 13 Dicembre 2016 il Gruppo di lavoro Articolo 29 per la Protezione dei Dati (nella formulazione inglese, usata anche in questo manuale, "Article 29 Data Working Party")[10] aveva emanato delle Linee guida[11] specificamente dedicate, comprensive anche di una serie di F.A.Q. per aiutare gli operatori del settore a orientarsi e recepire correttamente la nuova disciplina.

Un altro supporto utile è costituito dalle *Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato* adottate dal Garante per la privacy italiano[12] e dalla documentazione che viene pubblicata sul sito del Garante per la protezione dei dati personali, che ha dedicato una pagina intera al DPO, in continuo aggiornamento[13].

3. Chi deve dotarsi di un DPO?

Con riferimento al quesito riguardante chi debba dotarsi della figura del Data Protection Officer, occorre rifarsi a quanto stabilito dall'articolo 37 del GDPR.

Sulla base di quanto vi si legge, infatti, vi sono fondamentalmente tre circostanze particolari nelle quali è necessaria la nomina del DPO anche se, è bene sottolinearlo sin d'ora, può rivelarsi senz'altro opportuno provvedere alla nomina di questa figura anche al di fuori di quei casi in cui ciò sia considerato strettamente vincolante a livello normativo.

---

[10] Il Gruppo di lavoro articolo 29 per la protezione dei dati riuniva insieme le autorità garanti dei diversi Stati Membri dell'Unione Europea, sulla base di quanto stabilito dall'art. 29 della direttiva 95/46/CE ed è stato sostituito dall'European Data Protection Board in base a quanto previsto dal GDPR.

[11] Gruppo di lavoro Articolo 29, *linee guida sui responsabili della protezione dei dati,* adottate il 13 dicembre 2016, emendate in data 5 aprile 2017.

[12] Il Garante per la protezione dei Dati Personali ha pubblicato sia le *Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato (in aggiunta a quelle adottate dal Gruppo Art. 29 in Allegato alle Linee guida sul RPD)*, sia le *Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico (in aggiunta a quelle adottate dal Gruppo Art. 29 in Allegato alle Linee guida sul RPD)*.

[13] La pagina, denominata: "Il Responsabile della Protezione dei Dati (RPD)" è visionabile sul sito del Garante per la protezione dei dati personali all'URL: https://www.garanteprivacy.it/Regolamentoue/rpd.

Questa è, d'altronde, l'opinione che si ricava dai lavori del Gruppo di lavoro articolo 29, il quale nelle linee guida citate esplicita: **"anche ove il Regolamento non imponga in modo specifico la designazione di un RPD, può risultare utile procedere a tale designazione su base volontaria. Il Gruppo di lavoro "Articolo 29" (Gruppo di lavoro) incoraggia gli approcci di questo genere**"[14].

Ad ogni buon conto, i casi in cui si prevede l'obbligatorietà della figura del DPO sono quelli in cui:

a) "il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali" (art. 37, par. I, lett. a).

Ebbene, è del tutto evidente come tale definizione non consenta di rintracciare criteri di identificazione univoca degli "organismi pubblici" e delle "autorità pubbliche".

La molteplicità e la eterogeneità dei soggetti astrattamente riconducibili alle citate categorie ed esercenti una pubblica funzione rende infatti difficile comprendere nei casi concreti cosa sia o meno formalmente classificabile come soggetto pubblico ai fini del decreto.

Le linee guida del gruppo articolo 29 precisano solo che dovranno dotarsi di DPO tutti i soggetti che esercitano pubblici poteri[15].

Di conseguenza, diviene importante verificare come il diritto interno di ciascun Stato membro sia in grado di circoscrivere l'ambito di applicabilità del Regolamento riguardo a questo punto.

Su questa scia si è inserito quindi il Garante italiano, che in data 15 Dicembre 2017 ha emanato delle F.A.Q. specificamente dedicate all'ambito pubblico, in virtù delle quali sono da ritenersi vincolati alla nomina di un DPO i soggetti citati agli articoli 18 – 22 del D. lgs 196/2003[16].

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 re-

---

[14] Gruppo di lavoro articolo 29, *Linee guida sui responsabili della protezione dei dati*, cit., par. 1 (introduzione), p. 5.

[15] Gruppo di lavoro articolo 29, *Linee guida sui responsabili della protezione dei dati*, cit., par. 2.1.1, p. 8, che in nota richiama le definizioni di "ente pubblico" e "organismo di diritto pubblico" contenute nell'articolo 2, paragrafi 1 e 2, della direttiva 2003/98/CE del Parlamento europeo e del Consiglio, del 17 novembre 2003, relativa al riutilizzo dell'informazione del settore pubblico.

[16] Garante per la protezione dei dati personali, *Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico*, *cit.* par. 1

golare e sistematico degli interessati su larga scala" (art. 37, par. I, lett. b);

Anzitutto, non deve trarre in inganno l'espressione "attività principali", che potrebbe far intendere che il DPO sia una figura necessaria nel solo caso in cui il trattamento dei dati sia la prestazione tipicamente svolta all'interno di una struttura.

Così in effetti non è, dal momento che il senso di tale definizione sta nel prevedere l'obbligatorietà della nomina del DPO in tutti qui casi in cui il trattamento dei dati sia di fatto inscindibile dalla normale attività portata avanti dal titolare, configurandosi come *conditio sine qua non* per la liceità dei servizi resi[17].

Anche con riferimento al "monitoraggio regolare e sistematico degli interessi su larga scala", ci si deve interrogare sul reale significato di tale espressione.

Ancora una volta, quindi, è bene rifarsi alle linee guida del Gruppo di lavoro articolo 29.

Al punto 2.1.4. esse stabiliscono che con "regolare" si deve intendere quel tipo di trattamento che abbia almeno una delle seguenti caratteristiche:

- "avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
- ricorrente o ripetuto a intervalli costanti;
- che avviene in modo costante o a intervalli periodici.".[18]

Peraltro, sempre nello stesso paragrafo delle linee guida, si stabilisce che l'aggettivo "sistematico" debba intendersi riferito a quel trattamento che abbiano almeno una delle peculiarità di seguito indicate:

- "avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia"[19].

Si precisa che le forme di tracciamento e profilazione online sono da considerarsi senz'altro fra quei trattamenti che presentano un monitorag-

---

[17] *Cfr*. M. Maglio, *Il responsabile per la protezione dei dati personali* in M. Maglio, N. Tilli., M. Polini (a cura di), *Manuale di diritto alla protezione dei dati personali*, Maggioli Editore, 2017, p. 157.

[18] Gruppo di lavoro articolo 29, *Linee guida sui responsabili della protezione dei dati*, p. 2.1.4.

[19] *Ibidem*

gio regolare e sistematico dei dati, così da necessitare della nomina di un DPO.

Sul punto è bene chiarire che, contrariamente a quanto si è soliti pensare, trattamenti del genere possono aversi anche senza l'utilizzo delle più moderne tecnologie e della rete internet[20].

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" (art. 37, par. I, lett. c).

I dati in questione sono quelli idonei a rivelare "l'origine razziale o etnica di un soggetto, le sue opinioni politiche, convinzioni religiose, filosofiche o l'appartenenza sindacale"[21]. Inoltre, in questa fattispecie ci si riferisce anche a quei trattamenti che coinvolgano "dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona"[22]; inoltre l'art. 10 si preoccupa di sottolineare come il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza possa avvenire soltanto sotto il controllo della pubblica autorità.

4. Cosa si intende per "trattamento dati su larga scala"?

Come visto, un fondamentale riferimento operato dall'articolo 37, lettere b) e c) per individuare quali tipologie di trattamento siano idonee a far sorgere l'obbligo di nomina di un DPO, è il requisito della "larga scala".

Esso costituisce un ulteriore, fondamentale, presupposto su cui si fonda l'obbligo di dotarsi di un DPO e merita una particolare attenzione.

Anche la definizione di trattamento operato su "larga scala" tuttavia, di per sé considerato, risulta eccessivamente generico e soltanto operando un riferimento al considerando 91 si riesce a ricavare qualche maggiore informazione e a realizzare che tali sono quei trattamenti che *"mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato*"[23].

---

[20] *Cfr.* M. Maglio, *Il responsabile per la protezione dei dati personali*, op. cit. p. 158-159

[21] Art. 9, par.1, *Reg.* (*UE*) 2016/*679.*

[22] *Ibidem.*

[23] Cons. 91, *Reg.* (*UE*) 2016/*679.*