Guida per lo svolgimento della valutazione d’impatto sulla protezione dei dati (DPIA) - Parte II

Author : Redazione

Date : 1 Luglio 2020

Segue dalla prima parte

2.8 In quali trattamenti è necessaria la DPIA?

L’Art.35 punto 3 evidenzia, in particolare, tre prime tipologie di trattamento in cui **è sempre** richiesto lo svolgimento della DPIA:

Valutazione sistematica automatizzata dei dati (anche con profilazione) con effetti significativi sulle persone

Una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

Uso su larga scala di dati delle categorie particolari

Il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1 del Regolamento UE GDPR 679/16, o di dati relativi a condanne penali e a reati di cui all'articolo 10 del Regolamento;

Sorveglianza sistematica pubblica su larga scala

La sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Assieme a queste prime tre tipologie estremamente generali si deve, in prima istanza, certamente prendere in considerazione le tipologie più specifiche indicate dal Garante nazionale [Gar2] nel 2018, come anche tenere conto di quanto indicato, a livello Europeo, dal Working Party Art.29 [UE1]. Ai fini di assumere un atteggiamento **prudenziale** nell’analisi e di mirare ad una maggior ampiezza nella casistica descrittiva nella fase di *screening*, è qui proposto di integrare **anche alcuni aspetti indicati dal Garante UK ICO** [ICO1], fornendo questo secondo elenco più ampio e dettagliato.

Tale secondo elenco può considerarsi, alla luce degli approfondimenti nazionali e internazionali disponibili allo stato dell'arte, un riferimento adeguato per la fase di *screening*:

Trattamenti valutativi o di *scoring* su larga scala, nonché trattamenti che **comportano la profilazione degli interessati** nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato". [Gar2]

Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. *screening* dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi). [Gar2]

Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc. [Gar2]

Trattamenti su larga scala di dati aventi carattere estremamente personale [UE1]): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti). [Gar2]

Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti. [Gar2] [UE1] [UE2]

Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo). [Gar2]

Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi indossabili (*wearable*); tracciamenti di prossimità come ad es. il *wi-fi tracking*). [UE1] [Gar2]

Trattamenti che comportano lo scambio tra diversi Titolari di dati su larga scala con

modalità telematiche. [Gar2]

Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. *mobile payment*). [Gar2]

Trattamenti sistematici di dati biometrici (trattati per identificare univocamente una persona fisica) **e/o genetici**, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento. [UE1] [Gar2]

Trattamenti di categorie particolari di dati ai sensi dell'Art. 9 oppure di dati relativi a condanne penali e a reati di cui all'Art. 10 interconnessi con altri dati personali raccolti per finalità diverse. [Gar2]

Trattamenti che possono comportare un impedimento di esercizio di un diritto o di un servizio e/o contratto, cioè quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto" (Art. 22 e Considerando 91). Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto. Un esempio di ciò è rappresentato dal caso in cui una banca esamina i suoi clienti rispetto a una banca dati di riferimento per il credito al fine di decidere se offrire loro un prestito o meno. [UE1]

Trattamenti che possono comportare rischio di danni fisici, quando, cioè, il trattamento è di natura tale che una violazione dei dati personali potrebbe compromettere la salute fisica o la sicurezza fisica (*safety*) degli individui. [ICO1]

È opportuno sottolineare come, in ordine ai trattamenti di cui al precedente elenco, è stata svolta di recente dal *Comitato Europeo per la Protezione dei Dati* (**EDPB** = European Data Protection Board) in applicazione del **meccanismo di coerenza** previsto nel Regolamento, una intensa attività con le diverse Autorità di Controllo nazionali (come verificabile sul sito dell'EDPB [UE3]). Il lavoro svolto a livello EDPB ha condotto, ad esempio per l'Italia, alle osservazioni formali evidenziate in [UE2] che mostrano come a livello UE si propenda in questa fase ad una interpretazione meno restrittiva dell'obbligo della DPIA rispetto agli indirizzi assunti in prima istanza dal Garante nazionale, ma più in generale, anche dalle altre Autorità di Controllo nazionali. Tale dibattito resta sostanzialmente aperto tra il *Comitato Europeo per la protezione dei dati* e le *Autorità di Controllo nazionali* sull'interpretazione finale della norma e non è da escludere che le considerazioni qui svolte non debbano essere integrare e modificate in un futuro anche prossimo.

Ciò nonostante si **ritiene utile**, in questa fase ancora di sostanziale rodaggio di applicazione del Regolamento, **preferire prudenzialmente un approccio più conservativo**, che allarghi, come detto in precedenza, la casistica disponibile nella fase di screening.

Riferimenti al Regolamento per approfondimenti

Art.35 (punti 3 e 4) e Considerando n. 89, 90 e 91

2.9 Cosa significano per il Regolamento le parole chiave: nuove tecnologie, sistematico ed estensivo, effetto significativo, larga scala?

Le definizioni che seguono fanno riferimento agli studi internazionali svolti su questa materia e, come si osserverà, a volte si intersecano sovrapponendosi. Si ritiene comunque utile dare queste indicazioni e definizioni di massima affinché i Titolari del trattamento che operano nelle strutture pubbliche e private possano avere una linea di azione a cui fare, se del caso, riferimento.

Nuove tecnologie

Il Regolamento non definisce la nozione di *nuove tecnologie*, tuttavia oltre alla interpretazione letterale che si può immaginare come di *tecnologie precedentemente non disponibili per conoscenza e industrializzazione* (e quindi con conseguente mancanza di esempi già esistenti di applicazione nel trattamento di dati personali), il WP Art.29 suggerisce anche [UE1, UE4] l'interpretazione legata all'innovativa applicazione al trattamento dei dati personali di tecnologie già esistenti, quindi intendendo nuove modalità di utilizzo e di scopo delle stesse tecnologie.

Sistematico ed estensivo

Anche in questo caso il Regolamento non definisce in modo puntuale la nozione di *sistematico ed estensivo*. Ci può aiutare in questa definizione la Linea Guida Europea per i DPO [UE4] e il recente testo sempre derivato da progetti dell'UE [T4D1] sul trattamento dei dati personali, in cui si specifica che per trattamento *sistematico* si intende che:

- avviene in accordo ad un sistema, cioè con un approccio sistematizzato;
- è organizzato in modo metodico e dettagliato;
- è inserito in un piano più generale di raccolta dei dati;
- è condotto come parte di una strategia.

Il termine *estensivo*, invece, implica che il trattamento:

- ricopre un'ampia area geografica;
- coinvolge un ampio insieme di dati;
- comporta conseguenze su un gran numero di persone.

Effetto significativo

Il Regolamento non definisce la nozione di *effetto significativo*, tuttavia il WP Art.29 nei suoi documenti [UE1, UE4] indica come questa nozione si traduca in un impatto notevole sulle persone, potendo influenzare il loro *status*, il loro comportamento e le loro scelte ultime in modo rilevante.

Ad esempio si ha un *effetto significativo* di un trattamento quando questo, con i suoi effetti, può influenzare lo stato finanziario, la salute, la reputazione o altre caratteristiche economiche e/o

sociali delle persone.

Larga scala

Anche in quest'ultimo caso il Regolamento non definisce la nozione di '*su larga scala*', tuttavia fornisce un orientamento di merito nel Considerando 91 dove si specifica, dopo la locuzione *trattamenti su larga scala,* come questi mirino a gestire "*una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale… che potrebbero incidere su un vasto numero di interessati*".

Inoltre, il WP Art.29 raccomanda [UE1] di tenere conto, in particolare, dei seguenti fattori al fine di stabilire se un trattamento sia effettuato su *larga scala*:

- numero di soggetti interessati dal trattamento, in termini assoluti oppure espressi in percentuale della popolazione di riferimento;
- volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- durata, ovvero la persistenza, dell'attività di trattamento;
- portata geografica dell'attività di trattamento.

2.10 In quali casi esistono "eccezioni'"e si è esentati dallo svolgimento della DPIA?

Secondo le indicazioni fornite dal Gruppo Art. 29 [UE1], la DPIA non risulta necessaria, oltre che per trattamenti che non presentano rischio elevato per diritti e libertà delle persone fisiche, anche per trattamenti che:

- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo nazionale prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell'elenco facoltativo dei trattamenti eventualmente indicato dall'Autorità di controllo nazionale per i quali non è necessario procedere alla DPIA;
- fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

Alla luce delle disposizioni attuali disponibili anche a livello nazionale, nel seguito si considereranno questi quattro punti come le "eccezioni" operative da analizzare (vedi capitolo successivo).

2.11 Che ruolo svolge il Data Protection Officer nella conduzione della DPIA?

Il DPO supporta il Titolare nello svolgimento della DPIA. In termini generali, il DPO dovrebbe fornire consiglio e parere [T4D1, UE4] su:

- la necessarietà di eseguire una DPIA per uno specifico trattamento;
- la modalità di svolgimento della DPIA;
- quali misure di salvaguardia si possono adottare per mitigare gli eventuali rischi;

- l'esito finale della DPIA.

È opportuno che i consigli e le indicazioni fornite dal DPO sulla DPIA al Titolare vengano tracciate e documentate. Se il Titolare decidesse di operare in modo contrastante a quanto indicato dal DPO è necessario documentare nella DPIA le ragioni che inducono a tale decisione e assicurarsi di poter giustificare coerentemente scelte non condivise dal DPO.

Il DPO, inoltre, ha il compito di svolgere un'azione di monitoraggio nel tempo sulla DPIA e sulle azioni di mitigazione del rischio decise nella DPIA.

Riferimenti al Regolamento per approfondimenti

Art.35 (punto 2) e Art.39 (punto 1 a,c)

Ulteriori approfondimenti sul ruolo del DPO sono descritti in WP29 *Guidelines on Data Protection Officers*

2.12 Come è strutturata la DPIA proposta in questa Guida?

La modalità di svolgimento della DPIA descritta in questa Guida è graficamente rappresentabile con la fig.2.1 che segue.

Tale modalità recepisce - oltre ai dettami del Regolamento - tutti le indicazioni del Garante nazionale al momento disponibili, integrandole con i suggerimenti forniti dal WP Art.29 a livello europeo e con l'esperienza internazionale proposta, in particolare, dall'ICO (Autorità di Controllo del Regno Unito) e dal CNIL (Autorità di Controllo francese).

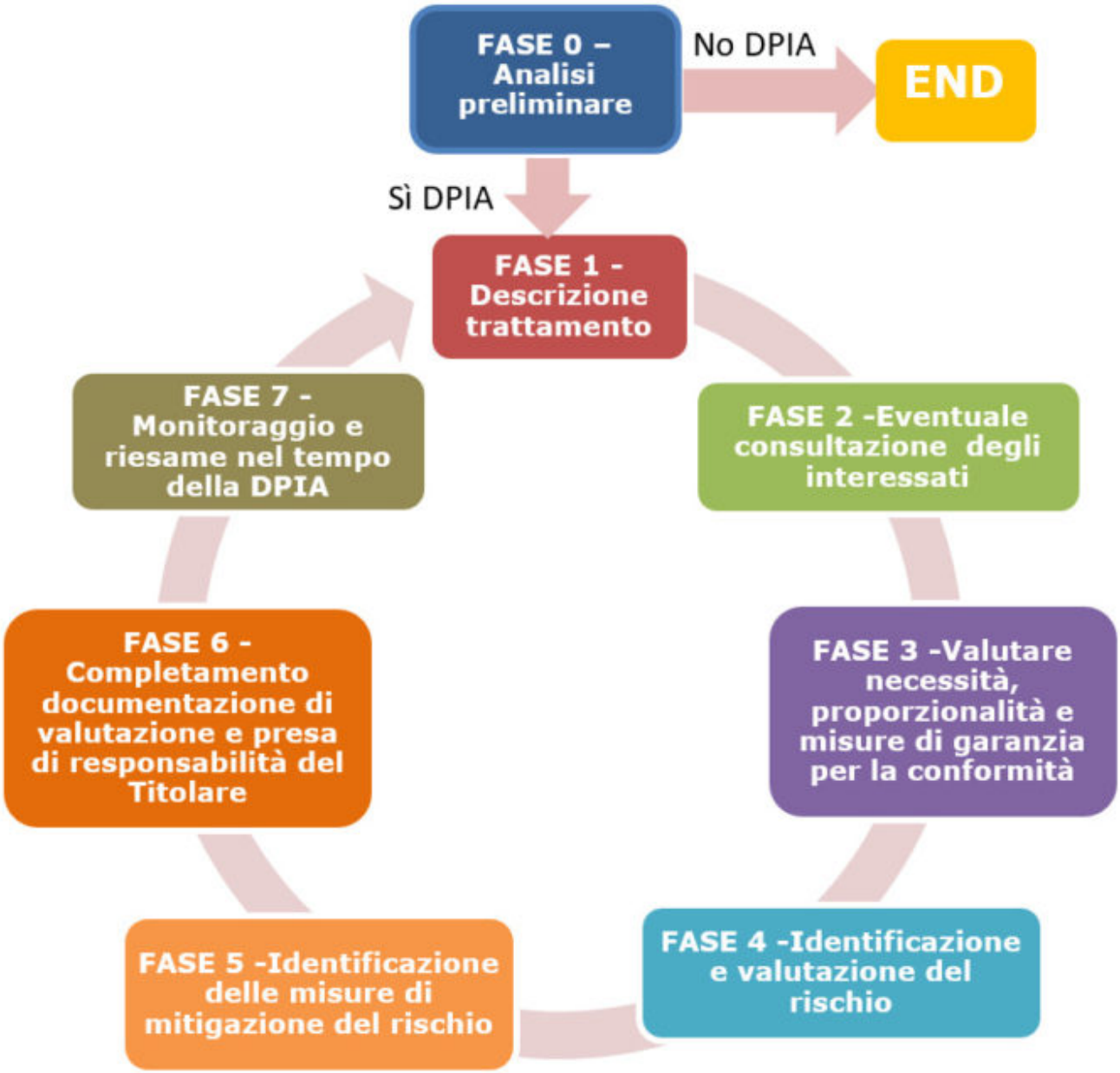

Fig. 2.1 – Rappresentazione grafica della strutturazione in 8 FASI della DPIA proposta nella Guida

La rappresentazione grafica presentata in Fig.2.1 è ripartita in fasi disgiunte che, partendo da una fase preliminare indicata come **Fase 0**, guidano il Titolare nella valutazione facendogli percorrere tutte le tappe logiche (corrispondenti a 7 ulteriori fasi) necessarie per svolgere una DPIA secondo i dettami delle norma e dello stato dell'arte nella materia.

Nei prossimi articoli, ognuna delle otto **fasi** qui rappresentate verrà discussa in dettaglio per fornire una guida, il più possibile chiara e esaustiva, nella valutazione.

Articolo a cura di **Marco Carbonelli**