Manuale RPD

Linee guida destinate ai Responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europea

(Regolamento (UE) 2016/679)

Elaborato per il programma "T4DATA" finanziato dall'UE

(Accordo di sovvenzione n°: 769100 — T4DATA — REC-DATA-2016/REC-DATA-2016-01)

di

Douwe Korff

Professore Emerito di Diritto Internazionale, Professore associato alla London Metropolitan University, alla Oxford Martin School e all'Università di Oxford

&

Marie Georges

Esperto indipendente sulla protezione internazionale dei dati
(Ex-CNIL, Ue, Consiglio d'Europa, ecc.)

Membri del Gruppo FREE - Fundamental Rights Experts Europe

Con il contributo del Garante italiano per la protezione dei dati personali & dei Partner del progetto

(versione approvata dalla Commissione, luglio 2019)

Il Manuale

Questo Manuale è stato redatto come parte del materiale di formazione del programma di per formatori "T4DATA", finanziato dall'UE e destinato al personale delle Autorità di protezione dei dati di alcuni Stati membri dell'UE (Data Protection Authorities - DPA), ed è finalizzato alla formazione dei Responsabili della Protezione dei Dati (RPD) operanti soprattutto nel settore pubblico, nell'adempimento degli obblighi loro incombenti ai sensi del Regolamento generale sulla protezione dei dati dell'UE (Regolamento 2016/679, RGPD). Il progetto è realizzato sotto l'egida dell'Autorità italiana della protezione dei dati, il *Garante per la protezione dei dati personali (nel prosieguo, "Garante" o "Garante della Privacy")*, e amministrato dalla *Fondazione Basso*, con l'ausilio di due esperti del Gruppo FREE - *Fundamental Rights Experts Europe*-, la Dott.ssa Marie Georges e il Professor Douwe Korff.

Il Manuale si è avvalso degli importanti contributi forniti dal Garante italiano e dalle altre autorità partner del progetto, che hanno fornito utilissimi esempi pratici e copie delle linee-guida rispettivamente elaborate sui temi attinenti il RGPD.

Si osservi che le note in calce riflettono, ove pertinente, le pregresse attività dei due esperti suddetti solo se si tratta di informazioni o materiali di dominio pubblico. Nel caso della dott.ssa Marie Georges ciò sarà meno frequente principalmente per la natura riservata o istituzionale dell'attività svolta per conto di organismi governativi nazionali e internazionali.

Per informazioni sul programma, i partner e gli esperti consultare il sito:
http://www.fondazionebasso.it/2015/wp-content/uploads/2018/04/T4Data_Brochure.pdf

Anche se elaborato per il programma "T4DATA", ci auguriamo che questo Manuale possa essere di aiuto a tutti coloro che sono interessati all'applicazione del Regolamento e, in particolare, ad altri RPD operanti nel settore pubblico o privato. Il testo è disponibile pubblicamente con licenza "Creative Commons" (CC).

Nota: poiché il Manuale è finalizzato alla formazione dei Responsabili per la Protezione dei Dati (RPD) nell'adempimento dei loro obblighi ai sensi del RGPD, è incentrato, soprattutto, sulla legislazione dell'UE in materia di protezione dei dati e, più specificamente, sulla legislazione di protezione dei dati di quello che in passato era denominato il "Primo Pilastro" ovvero sulle questioni del cosiddetto "mercato interno". Tuttavia, i paragrafi da 1.3.4 a 1.3.6 e da 1.4.3 a 1.4.5 contengono una breve trattazione delle norme e degli strumenti di protezione dati applicabili (attualmente o in precedenza) ad altri ambiti del diritto unionale – ossia, alle materie che in precedenza ricadevano nell'ambito del settore "giustizia e affari interni" (GAI) ovvero del "Terzo pilastro", quelle attualmente ricondotte all'area di "Libertà, sicurezza e giustizia"; alle materie relative alla cosiddetta politica estera e di sicurezza comune (PESC), l'ex "Secondo pilastro"; e alle attività delle istituzioni Ue in quanto tali. Il paragrafo 1.4.6. esamina anche le norme in materia di trasferimenti di dati in rapporto ai diversi quadri giuridici vigenti nell'Ue. Il Manuale, inoltre, non tratta la protezione dei dati all'esterno dell'UE/SEE, anche se è nostro parere che i RPD debbano avere un minimo di conoscenze sulla considerevole incidenza che le norme comunitarie hanno esercitato, e continuano ad esercitare, sulla protezione dei dati a livello mondiale. Auspichiamo di aggiungere questi aspetti in un secondo momento, in una versione riveduta del Manuale, il che permetterebbe anche un aggiornamento su informazioni attualmente non disponibili quali, ad esempio, gli sviluppi relativi al progetto di Regolamento e-Privacy che, al momento della stesura di questa edizione, è ancora in via di definizione attraverso il processo legislativo.

Il Manuale è disponibile anche nelle traduzioni in italiano, croato, bulgaro, polacco e spagnolo (le lingue dei partner del progetto).

In base alle disponibilità finanziarie, si potranno pubblicare anche traduzioni in altre lingue, in particolare in francese.

Prefazione

La prima edizione di questo "Manuale", scaturito dal progetto "T4Data – Training for Data" co-finanziato dall'Unione europea, pensiamo sia qualcosa di più e di diverso che non "un altro" manuale sul RGPD.

Si tratta, infatti, di un manuale dal taglio realmente pratico, la cui realizzazione è stata possibile, in primo luogo, grazie all'impegno e alla dedizione dei due esperti esterni che collaborano al progetto, la dott.ssa Marie Georges e il Prof. Douwe Korff, entrambi operanti da anni nei settori connessi ai diritti umani, alle tecnologie dell'informazione e della comunicazione, e alla protezione dei dati, in chiave sia teorica sia pratica. In secondo luogo, il manuale riflette i contributi scientifici e la competenza dei funzionari e dei rappresentanti delle cinque Autorità di controllo partner del progetto, che ne hanno arricchito significativamente i contenuti alla luce della pratica davvero quotidiana di queste tematiche.

Ma soprattutto, questo vuole essere uno strumento flessibile, espressione del diritto vivente, non già lettera morta. L'obiettivo di fondo è tradurre in indicazioni e raccomandazioni concrete, solide e ben documentate i compiti indubbiamente più onerosi legati al principio di responsabilizzazione fissato nel nuovo quadro normativo Ue, a loro volta intesi a garantire un approccio efficace alla protezione dei dati in un mondo caratterizzato da una vera e propria esplosione dei trattamenti di informazioni. Precisazioni e approfondimenti ulteriori potranno aggiungersi attraverso le attività di formazione e diffusione previste a livello nazionale durante il 2019, strutturate, appunto, sulla base dei contenuti del Manuale. I beneficiari del progetto e dei suoi prodotti sono i Responsabili della protezione dei dati, o RPD, e soprattutto i RPD operanti nel settore pubblico, che potranno servirsene per rafforzare e potenziare le competenze connesse alla gestione delle problematiche di protezione dati – a beneficio di tutti i soggetti coinvolti, siano essi titolari del trattamento, interessati o la società civile nel suo complesso.

Per questo le nostre cinque autorità hanno deciso di fare squadra per rendere possibile il progetto "T4Data", e sempre per questo motivo siamo particolarmente lieti di presentare il Manuale, un validissimo prodotto, disponibile in inglese e nelle cinque lingue dei partner, alle quali speriamo si aggiungerà presto anche una versione in francese, consapevoli che andrà a costituire un solido anello nella catena degli strumenti di cooperazione che stiamo forgiando giorno per giorno a livello europeo e mondiale.

Edyta Bielak–Jomaa, Presidente dell'Autorità polacca per la protezione dei dati

Mar España Martí, Direttore dell'Autorità spagnola per la protezione dei dati

Ventsislav Karadjov, Presidente della Commissione bulgara per la protezione dei dati personali

Anto Rajkovača, Direttore dell'Autorità croata per la protezione dei dati personali

Antonello Soro, Presidente, Garante per la protezione dei dati personali

INDICE

Pagina:

10 - Consulenza e monitoraggio della conformità delle politiche di protezione dei dati, dei contratti tra contitolari, tra titolari, e tra titolare e responsabile, norme vincolanti di impresa, e clausole per il trasferimento dei dati.

11 – Coinvolgimento nei codici di condotta e nelle certificazioni

Cooperazione con e consultazione dell'Autorità di protezione dati:

12 - Cooperazione con l'Autorità di protezione dati

Gestione delle richieste dell'interessato:

13 - Gestione delle richieste dell'interessato

Informazione e sensibilizzazione:

14 - Compiti di informazione e sensibilizzazione interna ed esterna

15 – Pianificazione e riesame delle attività del RPD

- o – O – o -

Linee guida destinate ai Responsabili della protezione dei dati operanti in ambito pubblico per garantire la conformità con il Regolamento generale sulla protezione dei dati dell'Unione europea

(Regolamento (UE) 2016/679)

Introduzione

Il 25 maggio 2018 è divenuto effettivamente applicabile il nuovo Regolamento Generale dell'UE sulla protezione dei dati (**RGPD** o "**il Regolamento**")[1] che ha sostituito la Direttiva sulla protezione dei dati del 1995 ("la Direttiva del 1995").[2] Adottato in risposta alla massiccia espansione del trattamento dei dati personali dall'introduzione della Direttiva del 1995 e allo sviluppo di tecnologie sempre più intrusive, il Regolamento prende le mosse dalla Direttiva e dalla giurisprudenza della Corte di Giustizia dell'Unione Europea (CGUE) ampliando significativamente la Direttiva e rafforzando considerevolmente l'attuale regime europeo di protezione dei dati. Sono molti i cambiamenti da registrare, dalla maggiore armonizzazione, al rafforzamento dei diritti dell'interessato, ad una più stretta cooperazione transfrontaliera fra le Autorità di protezione dei dati (DPA).

Fra i cambiamenti più rilevanti figurano l'introduzione del nuovo principio di "responsabilizzazione" e l'istituzione e la nomina di Responsabili per la protezione dei dati (**RPD**). I due elementi sono correlati perché i RPD saranno i responsabili dell'osservanza del principio di responsabilizzazione nelle istanze di cui fanno parte. Questo Manuale vuole essere un ausilio per tutti i nuovi RPD nell'espletamento delle loro funzioni nel settore pubblico.

Il Manuale si articola in tre sezioni:

- **La prima parte** presenta i concetti di "riservatezza", "privacy" e "protezione dei dati", le prime normative in materia di protezione dei dati, i principi e gli strumenti internazionali (in particolare, la Convenzione sulla protezione dei dati del Consiglio d'Europa del 1981), per poi passare alla discussione delle Direttive dell'UE sulla protezione dei dati nell'ambito del "Primo Pilastro" degli anni '90 e dell'inizio degli anni 2000, e presentare, infine, gli strumenti futuri di protezione dei dati, quelli di adozione più recente o in attesa di adozione (il RGPD, la proposta di Regolamento sulla

[1] Titolo completo: 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), G.U. L 119 del 4.5.2016, p. 1 e ss.:
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
Si osservi come, benché il Regolamento sia stato adottato nel 2016 e sia "entrato in vigore" giuridicamente parlando il 20mo giorno successivo alla sua pubblicazione nella GUUE, ossia il 25 maggio del 2016 (v. Art. 99, paragrafo 1), la sua "applicazione" (ossia, la sua effettiva applicazione) decorre dal 25 maggio 2018 (v. Art. 99, paragrafo 2).

[2] Titolo completo: Direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, G.U. L 281 del 23.11.1995, p. 31 e ss:
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en

e-Privacy e la Convenzione del Consiglio d'Europa "aggiornata")[3]. In questa prima parte non sono esaminati, per adesso, gli strumenti Ue creati negli anni '90 in materia di "terzo pilastro" né le norme in materia di protezione dati introdotte per le istituzioni dell'Ue stessa, o le disposizioni che nel tempo le hanno sostituite.*

***** Sperabilmente in una futura seconda edizione del Manuale sarà possibile dedicare a tali strumenti lo spazio che si meritano.

- **La seconda parte** fornisce un quadro di tutti gli elementi chiave del Regolamento generale sulla protezione dei dati prima di passare alla disanima del nuovo principio chiave della "responsabilizzazione" e alla figura e agli obblighi del Responsabile per la protezione di dati previsti dal RGPD;
- **La terza parte,** invece, tratteggia le linee guida per coadiuvare i RPD del settore pubblico a svolgere i numerosi compiti che li attendono, con una serie di esempi concreti che riguardano soprattutto tre settori principali: l'istruzione, la finanza e la sanità, il tutto correlato con esercizi pratici.

Oltre ad un ampio apparato di citazioni e link ai materiali di formazione nelle note a pié di pagina, il Secondo Volume del Manuale contiene un numeroso ed ampio materiale che è stato distribuito ai partecipanti delle formazioni "T4DATA".

Sito Web:

I materiali ed i link di cui sopra verranno resi disponibili, nella maggiore quantità possible, sul sito web (di libero accesso) che integra e accompagna questo Manuale (disponibile su licenza "Creative Commons"):

http://www.fondazionebasso.it/2015/t4data-training-data-protection-authorities-and-data-protection-officers/

[3] Per le restrizioni sulle problematiche discusse si veda la nota del riquadro "*Il Manuale*" a pag.1.

PARTE I

Origini e significato della protezione dei dati

Questa parte intende spiegare che cosa sia la protezione dei dati, come si sia sviluppata in Europa e come i nuovi e "moderni" strumenti di protezione dei dati si propongano di affrontare gli ultimi sviluppi tecnologici.

- La sezione 1.1 presenta i diversi concetti (nel caso di sovrapposizione) di riservatezza, privacy e vita privata e protezione dei dati, nonché l'approccio alla protezione dei dati sviluppato in Europa, compresi i diritti umani e i requisiti dello stato di diritto che, in Europa, sono alla base della protezione dei dati.
- La sezione 1.2 ripercorre le origini della protezione dei dati in Europa, l'emergere di principi e diritti di base in materia di protezione dei dati e lo sviluppo di strumenti normativi europei e mondiali, dapprima non vincolanti e poi vincolanti (la Convenzione sulla protezione dei dati e il Protocollo addizionale del Consiglio d'Europa del 1981).
- La sezione 1.3 esplora il modo in cui le norme e i principi sulla protezione dei dati sono stati sviluppati nel corso degli anni '90 e nei primi anni del nuovo secolo (per facilitare lo sviluppo del "Mercato interno" europeo che richiedeva sia la libera circolazione dei dati personali che la protezione del diritto fondamentale alla protezione dei dati), con particolare riguardo alla direttiva del 1995 sulla protezione dei dati (alla quale il Protocollo addizionale del 2001 alla Convenzione del 1981 intendeva allineare la Convenzione stessa) (paragrafi 1.3.1 e 1.3.2); in questa sezione viene inoltre trattata la normativa specifica applicabile al settore delle telecomunicazioni (paragrafo 1.3.3).

  I paragrafi finali di questa sezione illustrano sinteticamente gli strumenti di protezione dati negli ambiti precedentemente definiti "Giustizia e affari interni" (GAI) (paragrafo 1.3.4); nel settore della politica estera e di sicurezza comune (PESC) (paragrafo 1.3.5); e in rapporto alle istituzioni dell' Ue in quanto tali (paragrafo 1.3.6).
- La sezione 1.4 presenta i più recenti strumenti giuridici adottati per rispondere alle sfide future: il Regolamento generale dell'UE sulla protezione dei dati del 2016 (RGPD, applicabile dal 25 maggio 2018) (paragrafo 1.4.1) e la proposta di sostituzione della Direttiva UE sulla e-Privacy del 2002 con un Regolamento sulla e-Privacy.
- I successivi paragrafi di tale sezione illustrano in breve il principale e più recente strumento di protezione dati in quella che oggi è nota come l'area di Giustizia, libertà e sicurezza, ossia la direttiva del 2016 sulla protezione dei dati nelle attività giudiziarie e di polizia (paragrafo 1.4.3); la situazione in rapporto alla PESC (paragrafo 1.4.4); e un aggiornamento relativo allo strumento che disciplina la protezione dei dati trattati dalle istituzioni Ue, ossia il Regolamento 2018/1725 (paragrafo 1.4.5). Nel paragrafo 1.4.6 sono analizzati i meccanismi che presiedono ai flussi di dati fra i diversi quadri giuridici di riferimento nell'Ue.
- La Convenzione "aggiornata" del Consiglio d'Europa, aperta alla firma nel mese di ottobre 2018, è il tema dell'ultimo paragrafo di questa sezione (1.4.7).

  Al RGPD, in quanto oggetto primario del Manuale, sono dedicati ulteriori approfondimenti nella Parte II.

1.1 Riservatezza, privacy/vita privata e protezione dei dati: concetti diversi ma complementari nell'era della digitalizzazione

1.1.1 Riservatezza e Privacy/vita privata

Ambiti in cui le informazioni personali sono state subordinate a specifiche norme di **riservatezza** sono sempre esistiti. Gli esempi classici sono costituiti dal giuramento di Ippocrate del 4° secolo a.C. per la **professione medica,**[4] e dal "**sigillo della confessione**" per la Chiesa Cattolica romana .[5] In tempi più recenti, in particolare a partire dal XIX secolo, a **banchieri, avvocati,** altri **ministri del culto**, **lavoratori postali e delle telecomunicazioni** e molti altri professionisti è stato chiesto di trattare le informazioni ricevute in ambito lavorativo come riservate, privilegiate ,[6] o addirittura sacrosante.

Si tratta di doveri di riservatezza che, in generale, sono stati sempre visti come utili sia al singolo che alla società: il singolo aveva fiducia che la persona cui aveva confidato una certa informazione non la divulgasse e questa fiducia rafforzava il bene comune; il non rispetto della riservatezza poteva impedire, infatti, una richiesta di aiuto alle autorità o che le autorità venissero a conoscenza di certe informazioni mettendo così in pericolo la salute pubblica o altri vantaggi sociali. Pensiamo, ad esempio, al tentativo di limitare la diffusione di malattie sessualmente trasmissibili o a casi di estremismo religioso o politico.

Tuttavia, come spiega Frits Hondius, Vice-direttore dei diritti umani del Consiglio d'Europa incaricato della redazione della bozza del primo strumento di protezione dei dati vincolante a livello internazionale (la Convenzione sulla protezione dei dati del Consiglio d'Europa del 1981 di cui parleremo al punto 1.2.3, vedi *infra*), benché per certe categorie ci fosse un dovere

---

[4] Il giuramento di Ippocrate è stato attribuito ad Ippocrate (c. 460-370 a.C.) già nell'antichità, benché nuove scoperte dimostrino che potrebbe essere stato redatto dopo la sua morte. La versione più antica esistente è datata intorno al 275 d.C. e recita:
ἃ δ᾽ ἂν ἐνθεραπείῃ ἴδω ἢ ἀκούσω, ἢ καὶ ἄνευ θεραπείης κατὰ βίον ἀνθρώπων, ἃ μὴ χρή ποτε ἐκλαλεῖσθαι ἔξω, σιγήσομαι, ἄρρητα ἡγεύμενος εἶναι τὰ τοιαῦτα.
"Ciò che io possa vedere o sentire durante il mio esercizio o anche fuori dell'esercizio sulla vita degli uomini, tacerò ciò che non è necessario sia divulgato, ritenendo come un segreto cose simili.."
Si veda:
https://en.wikipedia.org/wiki/Hippocratic_Oath

[5] Nella Chiesa cattolica romana il "sigillo della confessione" o "sigillo sacramentale" è inviolabile. Si veda: https://www.catholiceducation.org/en/religion-and-philosophy/catholic-faith/the-seal-of-the-confessional.html

[6] Come sottolinea la Solicitors Regulation Authority (SRA), l'Autority che regolamenta avvocati e studi legali in Inghilterra e nel Galles, esiste (nel diritto anglosassone) una "differenza fra riservatezza e segreto professionale. In breve, mentre le informazioni riservate possono essere rivelate laddove ciò sia opportuno, il segreto è assoluto e le informazioni segrete non possono essere divulgate. Le comunicazioni riservate fra avvocato e cliente per ottenere o formulare un parere legale rientrano nel segreto professionale".
https://www.sra.org.uk/solicitors/code-of-conduct/guidance/guidance/Disclosure-of-client-confidential-information.page
In Francia, il segreto professionale (*secret professionnel*) di un avvocato (*avocat*) rientra nell'*ordre public*, ed è quindi assoluto, illimitato nel tempo, valido per ogni tipo di problematica legale qualunque ne sia la forma (scritta, elettronica, audio ecc.). Si veda:
http://www.avocatparis.org/mon-metier-davocat/deontologie/secret-professionnel-et-confidentialite

di riservatezza:[7]

> non esisteva un diritto corrispondente per pazienti, clienti o cittadini, di verificare l'accuratezza e la rilevanza dei dati che li riguardavano. E mentre esistevano sanzioni legali per punire gravi violazioni nel trattamento dei dati, nessuna legislazione forniva indicazioni utili su una corretta creazione e gestione degli archivi contenenti dati personali.

Il diritto alla "**privacy**" o al "**rispetto della vita privata**" è stato sancito solo nei Trattati internazionali sui diritti umani del secondo dopoguerra, come il Patto internazionale dell'ONU sui diritti civili e politici (ICCPR, Art. 17) e la Convenzione europea sui diritti umani (ECHR, Art. 8),[8] volta a tutelare soprattutto dalle illecite interferenze dello Stato nella vita privata del singolo, pensiamo alle intercettazioni delle comunicazioni da parte di organi di Stato[9] o la criminalizzazione di atti della sfera sessuale privata.[10] Tuttavia, tale diritto è stato anche interpretato dalla Corte EDU come richiesta allo Stato di protezione dei singoli contro la pubblicazione di fotografie scattate da soggetti privati, senza il consenso dell'interessato e in un contesto privato,[11] e contro le intercettazioni delle comunicazioni, in assenza di una base giuridica, da parte dei datori di lavoro.[12]

A ogni modo, mentre l'Art.8 dell'ECHR è stato di recente sempre più interpretato e applicato per proteggere i singoli nei loro dati personali e in relazione alla raccolta, l'utilizzo e la conservazione degli stessi, soprattutto se operati da parte dello Stato e di organismi di sicurezza nazionale,[13] negli anni '70 e '80 non era chiaro fino a che punto ci si potesse appellare al diritto alla vita privata nelle relazioni fra individui e fra individui ed organismi privati (il cosidetto problema dell'"effetto orizzontale dei diritti umani" o *Drittwirkung*)[14] – problema che, del resto, non ha ancora trovato una piena soluzione nella tradizionale legislazione sui diritti dell'uomo. I singoli, comunque, non possono far discendere dall'ECHR (o dall'ICCPR) un diritto di azione diretta contro altri singoli – il massimo che si possa fare è intraprendere un'azione legale contro lo Stato o l'organo di stato che non ha saputo

---

7 Frits Hondius, *A decade of international data protection*, in: Netherlands International Law Review, Vol. XXX (1983), pp. 103 – 128 (non disponibile online).

8 L'articolo 12 della Dichiarazione universale dei diritti umani del 1948, che è stata la "madre" sia dell'ICCPR che dell'ECHR (pur non essendo un trattato vincolante), recita: "Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza…" L'ICCPR e l'ECHR furono redatte parallelamente nel 1949-50 (ma l'ECHR, aperto alla firma alla fine del 1950, entrò in vigore nel 1953, vent'anni prima dell'ICCPR che fu aperto alla firma nel 1966 ed entrò in vigore solo nel 1976).

9 Ad es., CEDU, *Klass contro Germania*, sentenza del 6 settembre 1978.

10 Ad es., CEDU, *Dudgeon contro UK*, sentenza del 22 ottobre 1981.

11 Ad es., CEDU, *von Hannover contro Germania*, sentenza del 7 febbraio 2012.

12 Ad es., CEDU, *Halford contro UK*, sentenza del 25 giugno 1997.

13 Si veda la Scheda informativa – Protezione dei dati personali del Consiglio d'Europa, 2018: https://www.echr.coe.int/Documents/FS_Data_ENG.pdf
Una lista non esaustiva di cause della Corte europea dei diritti dell'uomo relative alla protezione dei dati personali è disponibile all'indirizzo:
https://www.coe.int/en/web/data-protection/echr-case-law
Per una discussione più generale si veda Lee A. Bygrave, *Data Protection Pursuant to the Right to Privacy in Human Rights Treaties*, International Journal of Law and Information Technology, 1998, volume 6, pp. 247–284, disponibile su:
https://www.uio.no/studier/emner/jus/jus/JUR5630/v11/undervisningsmateriale/Human_rights.pdf

14 Si veda Hondius, op.cit. (nota 7, vedi *supra*), p. 107, nel riferimento alla Relazione del Comitato esperti sui diritti umani, Consiglio d'Europa (DH/EXP(70)15).

proteggerli, ai sensi delle leggi nazionali, contro la loro azione.

Riassumendo: le legislazioni e le normative sulla riservatezza, il segreto professionale e la segretezza e le garanzie derivate dai diritti dell'uomo in materia di privacy e vita privata non hanno tutelato, e non tutelano, adeguatamente i singoli dalla raccolta e dall'utilizzo abusivo dei loro dati personali.

Per questo motivo, in tempi più recenti, è stato riconosciuto quale diritto separato e distinto il diritto alla "**protezione dei dati personali**" ("protezione dei dati") che ci accingiamo a trattare. Questo nuovo diritto *sui generis* deve sempre, naturalmente, essere inquadrato e letto nelle sue relazioni e nella sua complementarietà con i diritti tradizionali – come stabilito, in particolare sia dalla ECHR che dalla ICCPR: la protezione dei dati mira a garantire la piena ed efficace applicazione dei diritti tradizionali nel (relativamente) nuovo contesto digitale.

1.1.2 "Protezione dei dati"

I computer sono stati creati per scopi militari durante la **Seconda Guerra mondiale**. I decifratori britannici, guidati dal grande Alan Turing,[15] ne costruirono versioni primitive per decrittare i messaggi in codice tedeschi *Enigma e Lorenz*.[16] Negli USA, l'IBM, sotto la leadership del suo primo Amministratore delegato, Thomas J. Watson, produsse un gran numero di eleboratori dati per il settore militare cominciando la sperimentazione con computer analogici.[17] Anche i tedeschi usarono computer per il calcolo delle traiettorie dei missili *V2* [18].

Il bisogno di proteggere i diritti umani e le libertà nei regimi democratici in relazione al trattamento automatizzato dei dati personali è emerso solo più tardi quando, negli **anni '60,** i computer hanno cominciato ad essere usati a fini gestionali, sia nel settore pubblico che in quello privato. Per gli alti costi e lo spazio che occupavano all'epoca, solo i paesi più sviluppati investirono sullo sviluppo dei computer, e spesso solo a beneficio dei maggiori organismi pubblici e delle aziende. I primi utilizzi dei computer riguardavano il pagamento dei salari e dei fornitori, i registri dei pazienti negli ospedali, i censimenti pubblici e le statistiche – nonché gli schedari di polizia.

Alla luce di questi sviluppi, alla **fine degli anni '60/inizi anni '70**, si cominciò a parlarne anche in Germania (specialmente nel *Land* dell'Assia, per i registri di polizia), Norvegia, Svezia, Francia (soprattutto per la memoria delle atrocità commesse sulla popolazione e per registri pubblici compilati dagli occupanti nazisti nella Seconda Guerra mondiale), Regno Unito, USA,

---

15 Si veda:
http://www.maths.manchester.ac.uk/about-us/history/alan-turing/

16 Si veda: Chris Smith, *Cracking the Enigma code: How Turing's Bombe turned the tide of WWII*, 2 novembre 2017, su:
http://home.bt.com/tech-gadgets/cracking-the-enigma-code-how-turings-bombe-turned-the-tide-of-wwii-11363990654704
Il *Colosso,* usato per decodificare i messaggi *Lorenz* è in generale considerato "il primo computer programmabile, elettronico e digitale al mondo". Si veda:
https://en.wikipedia.org/wiki/Colossus_computer

17 Si veda:
https://en.wikipedia.org/wiki/Thomas_J._Watson

18 Si veda: Il computer analogico ed elettronico di Helmut Hoelzer utilizzato per i missili tedeschi V2 (A4) (testo prevalentemente in tedesco), all'indirizzo:
http://www.cdvandt.org/Hoelzer%20V4.pdf

ecc. – all'OCSE e al Consiglio d'Europa.[19] All'inizio i dibattiti si svolgevano tra esperti, vincolati da precisi obblighi etici (soprattutto negli USA, dove la classe medica e gli informatici furono i primi a dare alle stampe delle linee guida sulle "Procedure per la correttezza dell'informazione"),[20] e fra politici, preoccupati dei rischi di abuso, uso improprio o sicurezza dei dati trattati in modo automatizzato.

In seguito, **tra la metà e la fine degli Anni '70, inizio anni '80**, il dibattito si estese all'opinione pubblica; in Francia, già nel 1974, il catalizzatore fu una fuga di notizie sui piani del governo per la creazione di una banca dati a livello nazionale con un unico identificativo personale assegnato a ciascun cittadino e residente in Francia.[21] In Germania, la proposta di censimento nazionale nel 1983 fu accolta, in un clima politico di grande tensione, da una generale opposizione.[22] I dibattiti erano alimentati non soltanto dal rischio di violazione della privacy reso possibile dall'utilizzo delle nuove tecnologie, ma anche dalle conseguenze dell'uso di dati erronei e dalla possibile creazione di poteri autoritari frutto della centralizzazione della raccolta dei dati per scopi diversi e/o dall'utilizzo di identificativi unici per l'interconnessione dei file. In Europa questo portò alla richiesta di una "protezione dei dati" o "informatica e libertà" specifica e fondata su norme di diritto positivo (sostenuta da un sempre maggiore riconoscimento di tale esigenza da parte delle corti costituzionali e di altri supremi organi giurisdizionali), e all'adozione di strumenti internazionali (come vedremo al punto 1.2, vedi *infra*).

Il termine "protezione dei dati" (in tedesco: ***Datenschutz***) venne coniato per il titolo della primissima legge in materia, risalente al 1970, la Legge sulla protezione dei dati (*Datenschutzgesetz*) del Land tedesco dell'Assia, redatta dal "padre della protezione dei dati", il Professore Spiros Simitis.[23] Come sottolinea Burkert, il titolo utilizzava un termine

---

[19] Il Consiglio d'Europa ha adottato le prime Risoluzioni in materia nel 1973 e nel 1974: Risoluzioni del Comitato dei Ministri (73) 22 e (74) 29 (i link si trovano nelle note 39 e 40, vedi *infra*). Si veda anche la Relazione esplicativa alla Convenzione sulla protezione dei dati del Consiglio d'Europa del 1981, par. 6, consultabile all'indirizzo:
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434
I principi di applicazione di queste Risoluzioni figurano all'Allegato 1 del Manuale.

[20] Si veda: Robert Gellman, Fair Information Practices: A basic history, all'indirizzo:
https://bobgellman.com/rg-docs/rg-FIPshistory.pdf
Per molti anni, dagli anni '70 ai '90, Gellman ha lavorato alle problematiche legislative della privacy presso la Camera dei Rappresentanti statunitense.

[21] Si veda l'articolo del quotidiano Le Monde del 21 marzo 1974, "*SAFARI ou la chasse aux Français*" ("SAFARI, o la caccia ai francesi"), disponibile su:
http://rewriting.net/2008/02/11/safari-ou-la-chasse-aux-francais/
Il nome della banca dati, SAFARI, era un acronimo per "*Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus*" (Sistema automatizzato per i fascicoli amministrativi e la raccolta file sulle persone fisiche), ma fu anche scelto perché il Ministro incaricato del progetto all'epoca era un patito dei safari in Africa. La notizia venne ripresa da tutti i giornali nei giorni seguenti e il governo rinunciò al progetto poco tempo dopo nominando una Commissione *ad hoc* per lo studio del problema e la ricerca di soluzioni normative.

[22] Si veda: Marcel Berlinghoff, *Zensus und Boykott. Die Volkszählung vor 30 Jahren*, in: Zeitgeschichte-online, giugno 2013:
https://zeitgeschichte-online.de/kommentar/zensus-und-boykott-die-volkszaehlung-vor-30-jahren

[23] *Hessisches Datenschutzgesetz (HDSG) 1970*, in vigour dal 13 ottobre 1970, *Gesetz- und Verordnungsblatt für das Land Hessen, Teil I*, 1970, N. 41 (12 ottobre 1970), p. 625 e ss, testo originale (in tedesco) disponibile su:
http://starweb.hessen.de/cache/GVBL/1970/00041.pdf

"improprio, dal momento che [la Legge] non proteggeva i dati, ma il diritto degli individui i cui dati [venivano] trattati."[24]

Ma il termine rimase: il concetto – ormai notissimo in tutto il mondo (anche i francesi utilizzano l'espressione ***protection des données***) – è una definizione succinta per "protezione delle persone fisiche con riguardo al trattamento dei dati personali" (la locuzione usata sia nel titolo della Direttiva UE sulla protezione dei dati del 1995 che nel Regolamento generale dell'UE sulla protezione dei dati del 2016).[25] Anche se la locuzione è lunga ed articolata, non chiarisce del tutto il significato che gli europei le attribuiscono.

La protezione dei dati presenta sia aspetti attinenti alle libertà individuali che aspetti sociali.

In Francia, quindi, la protezione dei dati rientra nel dualismo delle tutele relative al singolo e di quelle relative alla società e alla costituzione, per cui:

> **L'informatica deve essere al servizio di ogni cittadino. … Non deve mettere in pericolo l'identità del singolo, i diritti umani, la vita privata, le libertà pubbliche o individuali.**[26]
>
> (Art. 1 del Testo di legge del 1978 *su Informatica, file e libertà*)

La legge francese suddetta ha acquisito rango costituzionale, e la giurisprudenza dei supremi organi giudiziari si fonda, a seconda delle questioni in gioco, sulla tutela della privacy o delle libertà.

In Germania, la protezione dei dati è vista soprattutto come una filiazione diretta del diritto fondamentale o (proto-diritto) al "[rispetto della] persona umana" (*das allgemeine Persönlichkeitsrecht*), garantito dall'Art. 2(1) della Costituzione, e strettamente collegato all'Art. 1(1). Partendo da questa base, la Corte Costituzionale, nella famosa sentenza *Censimento* del 1983, ha derivato un diritto più specifico di "**autodeterminazione informativa**" (*informationelle Selbstbestimmung*).[27] Risulta comunque evidente che il *Bundesverfassungsgericht* ricollega in modo chiaro e inequivocabile questo diritto individuale a più ampie e fondamentali norme sociali:[28]

> Un ordinamento sociale e giuridico in cui il cittadino sia all'oscuro di chi abbia informazioni su di lui, cosa si sappia, quando le informazioni sono state registrate e in che situazione si siano verificati atti, gesti o eventi della sua vita, è incompatibile con il diritto di autodeterminazione informativa. Una persona che abbia il dubbio che un comportamento inusuale sia osservato e, per questo, sistematicamente registrato, utilizzato o reso noto, cercherà di non attirare l'attenzione su di se. Qualcuno che, ed esempio, ritenga che la sua partecipazione ad una riunione o ad un'assemblea pubblica venga registata in maniera ufficiale, creando un pericolo per se, potrebbe decidere di non esercitare importanti diritti fondamentali ([come quelli garantiti agli] Articoli 8 e 9 della Costituzione). Questo non solo limiterebbe le possibilità di sviluppo personale del singolo, ma anche del bene commune, perché l'autodeterminazione è un requisito *sine*

---

[24] Herbert Burkert, Privacy-Data Protection: A German/European Perspective (privo di data, risalente circa al 2000), p. 46, disponibile su: http://www.coll.mpg.de/sites/www/files/text/burkert.pdf

[25] Il RGPD parla di "persone fisiche" invece di "individui".

[26] "*L'informatique doit être au service de chaque citoyen. ... Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.*" La frase, omessa, recita che "[La protezione dei dati] deve essere sviluppata nel quadro della cooperazione internazionale".

[27] BVerfG, 15.12.1983, BVerfGE Bd. 65, S. 1 ff. Sulla "autodeterminazione informativa", si veda § 151ff.

[28] *Idem*, § 154 (traduzione nostra).

> *qua non* per una società libera e democratica basata sulle capacità e la solidarietà dei cittadini.

Pur accettando volentieri la necessità di un diritto alla protezione dei dati, non tutti gli altri Stati europei che lo hanno inserito nelle rispettive Costituzioni come un diritto *sui generis* ,[29] hanno poi adottato il concetto tedesco dell'autodeterminazione informativa – spesso proprio per la troppa enfasi che questo porrebbe sull'aspetto della libertà individuale a discapito di più ampi diritti sociali.[30]

Come Hondius aveva già sottolineato nel 1983, possiamo comunque dire che in Europa tutti concordino sul fatto che:[31]

> La protezione dei dati è finalizzata alla salvaguardia di un equo e ragionevole equilibrio fra gli interessi dei singoli e quelli della comunità [per quanto riguarda il trattamento dei dati personali].

Gli Stati europei hanno adottato una posizione per cui, allo scopo di raggiungere l'auspicato equilibrio, si devono rispettare i seguenti **principi normativi**:

- la raccolta e il conseguente uso e diffusione dei dati personali devono essere regolamentati per **legge** (ad es., con **norme giuridiche vincolanti**, piuttosto che con codici volontari o linee guida non vincolanti);[32]
- tali leggi dovrebbero essere **"leggi omnibus"** applicabili, in principio, a tutti gli organismi pubblici e privati che si occupano del trattamento dei dati personali (con le eccezioni e le modifiche del caso, come previsto da norme specifiche e in caso di necessità, ma sempre nel rispetto dello "spirito essenziale" della legge);
- la normativa in questione deve contenere determinate **norme di diritto sostanziale** (che riflettano il nucleo essenziale dei principi, "**della protezione dei dati** di cui parleremo nel prossimo capitolo) e garantire, ai soggetti cui si riferiscono i dati personali, **diritti individuali fondamentali**; inoltre l'applicazione di tali leggi dovrebbe essere oggetto **di controllo da parte di appositi organismi di vigilanza** (generalmente denominati **Autorità della protezione dei dati o Data Protection Authority -DPA).**

---

[29] Cfr. la legge austriaca sulla protezione dei dati del 1978 che contiene, all'Art. 1, una norma "costituzionale" in cui si dichiara che la protezione dei dati personali è un diritto protetto dalla Costituzione. La protezione dei dati è espressamente prevista anche nelle Costituzioni di Spagna (Art. 18-4), Portogallo (Art. 35), Grecia (Art. 9A), Ungheria (Art. 59), Lituania (Art. 22), Slovenia (Art. 38), Slovacchia (Art. 19) e Paesi Bassi (Art. 10).

[30] Si veda, ad es., il blog *Informationelle Selbstbestimmung - (noch) kein neues Grundrecht*, 26 ottobre 2017, sul rifiuto della Camera bassa del Parlamento federale svizzero (*Nationalrat*) di sancire il principio di autodeterminazione informativa nella Costituzione federale svizzera:
https://www.humanrights.ch/de/menschenrechte-schweiz/inneres/person/datenschutz/informationelle-selbstbestimmung
Nemmeno nei Paesi Bassi il principio è stato adottato nella legislazione o negli ordinamenti giurisprudenziali-sebbene e nonostante questo, la Corte suprema, la *Hoge Raad*, sia stata influenzata dalla giurisprudenza della Corte costituzionale tedesca. Si veda: T. F. M. Hooghiemstra, Tekst en toelichting Wet bescherming persoonsgegevens (2001), sezione 4.3 (p. 18).

[31] Hondius, op.cit. (nota 7, vedi *supra*), p. 108.

[32] Cfr. l'interpretazione del concetto di "legge" nella Convenzione europea dei diritti dell'uomo (in particolare gli Articoli 8 – 11) della Corte europea dei Diritti dell'Uomo.

1.2 Le prime norme di protezione dei dati, principi e strumenti internazionali[33]

1.2.1 Le prime norme di protezione dei dati

"L'Europa occidentale è la culla della protezione dei dati"[34]

Come già ricordato, la primissima legge al mondo sulla protezione dei d**ati è stata la *Datenschutzgesetz* del Land tedesco dell'Assia, adottata nel settembre 1970.**[35] La legge introdusse anche il primo Organismo indipendente di vigilanza della protezione dei dati (sebbene riservato, per ragioni di competenza dello Stato, al solo settore pubblico e con limitati poteri di mediazione e non di applicazione).

In quello stesso decennio, alla Legge di protezione dei dati dell'Assia seguirono, in Europa, l'adozioni di leggi di protezione dei dati nazionali (valide in tutto il territorio dei rispettivi Stati) in **Svezia (1973)**, la prima **Legge federale tedesca sulla protezione dei dati (alla fine del 1977)** (che riguardava il trattamento dei dati personali da parte di organismi federali e del settore privato), **la Legge francese *Informatica e Libertà* del 6 gennaio 1978**, leggi in **Austria**, **Danimarca**[36] **e Norvegia (tutte del 1978)** e **Lussemburgo (1979)**. Sebbene alcune contenessero, come la Legge federale tedesca, norme specifiche per i settori (federali) pubblici e privati, si tratta di "leggi omnibus", perché entrambi i settori sono disciplinati secondo gli stessi principi e diritti di base, spesso di derivazione costituzionale.[37]

1.2.2 I principi di base

Le leggi varate negli anni '70 in Europa si sono articolate intorno a quello che potremmo definire, con un termine di ampio respiro, un **"nucleo" di principi e di diritti,** sempre più riconosciuti da tutti e simili ai principi di base delle *Procedure per la correttezza delle*

---

[33] Per i dettagli storici, con riferimento specifico alla redazione in parallelo delle Linee Guida dell'OCSE nel 1980 o della Convenzione sulla protezione dei dati del Consiglio d'Europa nel 1981, e sull'emergere, già all'epoca, di posizioni diverse fra Europa e USA, si veda: Frits Hondius, op.cit. (nota 7, vedi *supra*), pp. 103 – 128, e la Relazione esplicativa alla Convenzione sulla protezione dei dati del Consiglio d'Europa, op.cit. (nota 19, vedi *supra*), par. 14. Una panoramica generale molto utile sugli sviluppi storici della privacy si trova al Capitolo 4 del Quadro di riferimento sulla privacy dell'OCSE, intitolato *Il mondo privacy in evoluzione a 30 anni dalle line-guida sulla privacy dell'OCSE*, di cui parleremo in seguito (si veda la nota 41). Un resoconto personale molto interessante sui retroscena della stesura delle Linee Guida dell'OCSE, gli orientamenti politici (Europa contro USA) e le personalità coinvolte (fra le quali Frits Hondius, Louis Joinet, Stefano Rodotà e Spiros Simitis), si può leggere in Michael Kirby, Privacy Today: Something Old, Something New, Something Borrowed, Something Blue, Journal of Law, Information and Science, 2017 25(1), disponibile all'indirizzo: http://www.austlii.edu.au/au/journals/JlLawInfoSci/2017/1.html

[34] Hondius, op.cit. (nota 7, vedi *supra*), p. 104, per il riferimento alle prime leggi di cui si parla nel testo.

[35] Si veda la nota 23, vedi *supra*. Per maggiori dettagli sulla storia della protezione dei dati in Germania si rimanda a: Herbert Burkert, op.cit. (nota 24, vedi *supra*).

[36] In Danimarca, furono approvate nello stesso giorno due leggi, una per il settore privato e l'altra per quello pubblico (Leggi n° 293 e 294, dell'8 giugno 1978) entrambe basate, comunque, sugli stessi ampi principi. Per gli antecedenti si veda l'*Introduzione* in: Peter Blume, Personregistrering, Copenhagen, 1991. Le due leggi rimasero in vigore, con vari emendamenti, fino al 2000, quando venne approvata una nuova legislazione per il recepimento della Direttiva sulla protezione dei dati dell'UE del 1995.

[37] Le leggi sulla protezione dei dati vigenti nei singoli Laender (Landesdatenschutzgesetze) si applicano al settore pubblico, ma si basano su identici principi che trovano fondamento nella Costituzione.

informazioni redatte, circa nello stesso periodo, negli USA (benché queste fossero meno dettagliate e non vincolanti).[38]

I principi base enucleati in queste prime leggi in Europa trovarono un riflesso nei **primi strumenti europei (non-vincolanti)** in materia ad opera del Consiglio d'Europa (e che diventeranno più tardi la base della Convenzione, questa volta vincolante, sulla protezione dei dati del Consiglio d'Europa):

- 1973: Risoluzione del Consiglio d'Europa (73)22 sulla Tutela della riservatezza delle persone in rapporto alle banche dati elettroniche nel settore privato, adottata dal Comitato dei Ministri il 26 settembre 1973;[39]
- 1974: Risoluzione del Consiglio d'Europa (74)29 sulla Tutela della riservatezza delle persone in rapporto alle banche dati elettroniche nel settore pubblico, adottata dal Comitato dei Ministri il 20 settembre 1974.[40]

I principi "fondamentali" furono poi riconosciuti in **strumenti internazionali globali, ma non ancora vincolanti**, quali:

- Le Linee-guida sulla protezione della vita privata e sui flussi transfrontalieri di dati personali dell'OCSE del 1980;[41] e
- I Principi guida per la regolamentazione dei file di dati personali computerizzati dell'ONU del 1989, adottati dall'Assemblea Generale dell'ONU (UNGA).[42]

Per quanto riguarda il testo completo dei principi fondamentali negli strumenti internazionali non vincolanti databili fra gli anni '70 e gli anni '80 e di cui sopra, nonché i principi della *Procedura per la correttezza delle informazioni* degli USA del 1973, rimandiamo ai link ipertestuali di cui in nota.

Qui ci limitiamo a sottolineare che tutti mirano ad affrontare un problema intrinseco all'impiego dei computer: per sua stessa natura, il computer facilita molte e nuove utilizzazioni dei dati, anche di quelli personali, senza che a ciò si accompagni necessariamente

---

38 Si veda la sotto sezione 1.3.4, *infra*.

39 Disponibile all'indirizzo: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805028 30

40 Disponibile all'indirizzo: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d1c 51

41 OCSE, Raccomandazioni del Consiglio riguardanti linee guida sulla protezione della vita privata e sui flussi transfrontalieri di dati personali, 23 settembre 1980, disponibile su: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonal data.htm
Per gli antefatti, si veda Kirby, op.cit. (nota 33, *supra*).
Va sottolineato che le Linee-Guida dell'OCSE vennero rivedute nel 2013 nell'ambito della creazione di un più ampio *Quadro di riferimento sulla vita privata* dell'OCSE, che include nuove norme per l'attuazione della cooperazione sulla vita privata rifacendosi ad una Raccomandazione in materia del 2007; si veda: https://www.oecd.org/sti/ieconomy/privacy.htm
Il nuovo testo, comunque, non inficia i principi fondamentali del testo del 1980.

42 ONU, Principi guida per la regolamentazione dei file di dati personali computerizzati, UNGA Ris. 44/132, 44 UN GAOR Supp. (N°. 49) in 211, UN Doc. A/44/49 (1989), disponibile su: https://www1.umn.edu/humanrts/instree/q2grcpd.htm
Si tratta del primo strumento che riconosce la necessità di un'Autorità indipendente sulla protezione dei dati.

l'attenzione ad aspetti di sicurezza o a possibili limitazioni dell'uso. In altri termini, questi principi fondamentali intendono prevenire abusi dell'utilizzazione dei dati personali che risultano fin troppo facilitati dalle nuove tecnologie in assenza di controlli. In questa prospettiva, i principi suddetti mantengono la loro significatività.

Per citare quanto previsto nelle Linee-guida dell'OCSE:

Principi OCSE del 1980

Principio di limitazione della raccolta dei dati

Devono essere posti dei limiti alla raccolta dei dati personali e tali dati devono essere ottenuti in modo corretto e lecito, laddove opportuno, con la conoscenza o il consenso del soggetto cui i dati si riferiscono.

Principio della qualità dei dati

I dati personali debbono essere pertinenti allo scopo di utilizzo e, nella misura necessaria a tali fini, devono essere completi, esattii e mantenuti aggiornati.

Il principio della specificità dello scopo

Le finalità per cui vengono raccolti i dati personali devono essere specificate al più tardi al momento della raccolta dei dati ed il loro utilizzo deve essere limitato all'adempimento di tali finalità o ad altre finalità che non risultino incompatibili con quelle iniziali, secondo quanto specificato ogniqualvolta intervenga una modifica delle finalità stesse.

Il principio della limitazione d'uso

I dati personali non possono essere divulgati, resi disponibili o utilizzati per scopi diversi da quelli specificati [dal precedente principio] ad eccezione:

a) di quelli per i quali si è ottenuto il consenso dell'interessato; o

b) per effetto di disposizioni normative.

Il principio di salvaguardia della sicurezza

I dati personali devono essere protetti adottando ragionevoli misure di sicurezza contro rischi quali la perdita o l'accesso non autorizzato, la distruzione, l'utilizzo, la modifica o la divulgazione dei dati stessi.

Il principio di apertura

Deve essere prevista una politica generale di apertura sugli sviluppi, le prassi e le politiche relative ai dati personali. Devono essere approntati e resi disponibili mezzi che permettano di confermare l'esistenza e la natura dei dati personali, lo scopo principale del loro utilizzo, nonché l'identità e la residenza abituale del titolare del trattamento.

Il principio di partecipazione individuale

Ogni persona deve avere il diritto:

a) di ottenere dal titolare del trattamento, o in altro modo, la conferma o la smentita che il titolare sia in possesso di dati che lo riguardano;

b) di ricevere comunicazione di dati che lo riguardano entro un lasso di tempo ragionevole; con costi, qualora ve ne siano, non eccessivi; in maniera ragionevole e in una forma pienamente comprensibile dal soggetto;

c) di ottenere spiegazioni, se una richiesta inoltrata ai sensi dei sottoparagrafi(a) e (b) non viene accolta, e di impugnare il rigetto;

d) di contestare i dati che lo riguardano e, se la contestazione viene accolta, ottenerne la cancellazione, la rettifica, il completamento o la modifica.

Il principio di responsabilizzazione

Il titolare del trattamento deve essere considerato responsabile del rispetto delle misure che danno attuazione ai principi di cui sopra.

E' importante rilevare che i principi (in tutti gli strumenti considerati) devono sempre essere letti e applicati insieme: solo così, infatti, possono offrire una valida protezione contro ogni uso improprio o abuso dei dati personali quali errori nei dati immagazzinati o digitalizzati, raccolta di un numero di dati maggiore del necessario, conservazione dei dati per un tempo maggiore del necessario, utilizzo dei dati per finalità diverse, furto o divulgazione di dati a terzi per scopi illegali, perdita di dati, hacking ecc., ecc.

1.2.3 La Convenzione sulla protezione di dati del Consiglio d'Europa del 1981 e il Protocollo addizionale

Il primo strumento internazionale vincolante nel campo della protezione dei dati è stata la Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale del Consiglio d'Europa del 1981, meglio nota come Convenzione sulla protezione dei dati (CPD) o "Convenzione N°108" dalla numerazione della Serie dei Trattati Europei.[43] Come Convenzione del Consiglio d'Europa (piuttosto che una "Convenzione europea"), la Convenzione sulla protezione dei dati è aperta alla firma, su invito (Art.23), anche di Stati che non sono membri del Consiglio d'Europa. Ad oggi (agosto 2018), la Convenzione è stata ratificata da tutti i 47 Stati membri del Consiglio d'Europa e da sei Stati extra-europei (Uruguay [2013], Mauritius [2016], Senegal [2016], Tunisia [2017], Capo Verde e Messico [2018]).[44] Altri due Stati non-europei sono stati invitati a ratificare la Convenzione: Argentina e Burkina Faso.[45] Nel 2001, la Convenzione è stata ampliata da un Protocollo addizionale.[46]

La Convenzione del 1981 ed il Protocollo addizionale sono brevemente descritti (vedi *infra*) al passato perchè, più di recente, nel 2018, sono stati radicalmente emendati ("aggiornati") in un nuovo protocollo, come vedremo nella sezione 1.3. Va comunque sottolineato che la Convenzione rivista ("aggiornata") sarà applicabile solo per gli Stati o gli organismi firmatari; per gli altri rimane di applicazione il testo del 1981 (con il Protocollo aggiuntivo del 2001 laddove di applicazione).

---

43 Titolo completo: Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale del Consiglio d'Europa, aperto alla firma a Strasburgo il 28 gennaio 1981, CETS N° 108, disponibile su:
https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

44 Si veda:
https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/108/signatures?p_auth=qsJbzlEi

45 *Idem*.

46 Titolo completo: Protocollo addizionale alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale, concernente le autorità di controllo ed i flussi transfrontalieri del Consiglio d'Europa, aperto alla firma a Strasburgo l'8 novembre 2001, CETS N° 181, consultabile su:
https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680080626
Il Protocollo addizionale è stato ratificato da 36 Stati membri del Consiglio d'Europa su 47 e da sei Stati non-membri (Cabo Verde, Mauritius, Messico, Senegal, Tunisia e Uruguay). Il Burkina Faso è stato invitato a sottoscrivere. Si veda:
https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/181/signatures?p_auth=yDDCP83k

In qualità di strumento internazionale vincolante, la Convenzione del 1981 (a differenza dei precedenti strumenti non vincolanti) doveva includere, e utilmente lo fece, **definizioni** giuridiche più precise dei concetti fondamentali della legislazione sulla protezione dei dati personali: "**dati personali**", "**titolare del trattamento**" e "**trattamento**" (sebbene, in successivi strumenti vincolanti, tali concetti ebbero bisogno di ulteriori articolazioni e furono oggetto di ampliamenti e aggiunte), (Art. 2).

I principi fondamentali sulla protezione dei dati di cui abbiamo parlato prima – i **Principi di limitazione della raccolta, qualità dei dati, specificità di scopo e limitazione d'uso** – figurano all'Art.5 della Convenzione del 1981 (pur non utilizzando gli stessi termini: la Convenzione, infatti, elenca questi principi al capitolo intitolato "*Qualità dei dati*"). Il **Principio di sicurezza dei dati** (di cui si parla nella Convenzione come *Principio di salvaguardia della sicurezza*) è stato specificato all'Art.7; quelli di **Apertura e di partecipazione individuale** figurano all'Art. 8 (al capitolo "*Salvaguardie aggiuntive per i soggetti interessati*").[47]

La Convenzione ha aggiunto anche un articolo specifico sul trattamento di "**categorie speciali di dati**", cioè "*i dati personali che rivelano le origini razziali, le opinioni politiche, le convinzioni religiose o altre convinzioni, nonché i dati a carattere personale relativi alla salute o alla vita sessuale*" e "*i dati a carattere personale relativi a condanne penali*" (Art. 6). Si sancisce che questi dati – più comunemente denominati "**dati sensibili**" – "*non possano essere elaborati automaticamente a meno che il diritto nazionale non preveda appropriate garanzie*".

NB: la necessità di norme speciali per determinati tipi di dati fu, all'epoca, al centro di un aspro dibattito. Alcuni, fra cui Simitis, ritenevano che ogni dato potesse essere considerato sensibile a seconda del contesto, mentre altri dati in elenco potevano, in un contesto diverso, non essere considerati sensibili. Altri ritenevano che solo i dati sensibili avessero bisogno di regolamentazione per la loro pericolosità intrinseca ed il potenziale discriminatorio. Alla fine, la proposta avanzata da Louis Joinet, rappresentante francese e Presidente del Comitato del Consiglio d'Europa incaricato della stesura,[48] prevalse, e tutti i dati personali vennero disciplinati, con un maggiore livello di protezione per quelli considerati sensibili.

Contemporaneamente, la Convenzione permetteva agli Stati firmatari l'adozione di **eccezioni e restrizioni** alla maggior parte dei dispositivi della Convenzione (ma non ai requisiti di sicurezza dei dati), al fine di tutelare "***la sicurezza dello Stato, la sicurezza pubblica, gli interessi monetari dello Stato o la repressione dei reati***" oppure "***la persona interessata o i diritti e le libertà di terzi***", a patto che la deroga fosse "prevista dalla **legge** dello Stato" e

---

[47] L'applicazione dei diritti fondamentali, infatti, rappresenta la garanzia principale di protezioine delle persone fisiche: i diritti dei soggetti interessati sono complementari agli altri perché permettono un maggior controllo da parte dell'interessato e l'applicazione a singoli casi.

[48] Louis Joinet fu, fino al pensionamento, un giurista francese membro della Commissione *ad hoc* incaricata della stesura della Legge francese sulla protezione dei dati del 1978, prima di diventare il primo direttore della DPA francese (la Commissione Nazionale Informatica e Libertà-CNIL). Responsabile della stesura delle Linee Guida dell'ONU (nota 41, vedi *supra*) fu un esimio rappresentante del Governo francese presso il Comitato dei diritti umani dell'ONU. Si veda:
https://fr.wikipedia.org/wiki/Louis_Joinet
http://www.liberation.fr/societe/2013/12/18/louis-joinet-le-hessel-de-la-justice_967496

"costituisse una misura ***necessaria [e proporzionata]*** in una società democratica" per la tutela di tali interessi (Art. 9(2)).[49]

Oltre ad aver conferito valore giuridico ai principi fondamentali della protezione dei dati (con l'aggiunta delle norme speciali sui dati sensibili) e ai diritti dei soggetti interessati, la Convenzione del 1981 confermò anche due dei **requisiti normativi** europei cui abbiamo accennato prima:

- ha confermato agli Stati firmatari di applicare le disposizioni adottando **norme giuridicamente vincolanti** che possono prendere la forma di leggi statutarie, regolamenti o norme amministrative ed essere completate da linee guida o codici non vincolanti – fermo restando che le norme fondamentali devono sempre costituire "misure vincolanti";[50]
- ha confermato agli Stati firmatari un'applicazione della legge di ampio respiro, **a (tutte) "le raccolte automatizzate di dati a carattere personale e all'elaborazione automatica degli stessi nel settore pubblico e privato"** (Art. 3(1)). In altre parole, almeno in linea di principio, si impone l'adozione di **"leggi omnibus"**.[51]

La Convenzione del 1981, comunque, non imponeva ancora agli Stati firmatari la creazione di un'**Autorità** indipendente **sulla protezione dei dati personali** né affrontava un problema destinato ad assumere un rilievo sempre maggiore alla luce del continuo aumento dei flussi internazionali di dati: **la necessità di limitare tale flusso** allo scopo di impedire l'elusione delle norme fondamentali e la negazione di diritti cruciali per il soggetto interessato, imponendo norme che ne garantissero la tutela anche dopo che i dati avessero lasciato il territorio di uno Stato.

La Convenzione del 1981 sanciva solamente che gli Stati firmatari:

> Non possono, al solo fine della protezione della vita privata, proibire o sottoporre a un'autorizzazione speciale i flussi attraverso i confini di dati a carattere personale destinati al territorio di un altro Stato (Art. 12(2)),

a meno che lo Stato in questione non prevedesse una regolamentazione specifica per certe categorie di dati, o che il trasferimento ad altri Stati fosse effettuato con l'intenzione di aggirare la legislazione dello Stato in questione (Art. 12(3)).

In altri termini, la Convenzione del 1981 non disciplinava il trasferimento dei dati personali verso il territorio di uno Stato non contraente.

Va infine rilevato che la Convenzione si applicava solamente alle "raccolte automatizzate di dati personali e all'elaborazione automatica di tali dati" (Art. 3(1), si veda anche l'Art. 1). I **casellari manuali**, quindi, compresi i "casellari manuali strutturati", non venivano disciplinati (sebbene gli Stati firmatari avessero facoltà di estendere l'applicazione della Convenzione a tali file: Art. 3(2)(c)).

---

[49] Nella CEDU, il requisito della proporzionalità è ricavabile dal requisito espresso di necessità (in una società democratica), mentre nel diritto UE (in particolare, nella Carta dei diritti fondamentali dell'Unione europea) i due concetti rappresentano principi distinti seppur strettamente connessi (v. Art. 52 della Carta suddetta).

[50] Relazione esplicativa alla Convenzione del Consiglio d'Europa, op.cit. (nota 19, vedi *supra*), par. 39.

[51] È lo Stato firmatario che, al momento della stipula, può comunicare che "non applicherà la Convenzione a certe categorie di raccolte automatizzate di dati a carattere personale" (Art. 3(2)(a)).

Due di queste mancanze sono state corrette nel Protocollo addizionale relativo alle Autorità di controllo e ai flussi transfrontalieri di dati, adottato nel 2001 (già menzionato),[52] che, come indicato nel titolo, impone la creazione di **DPA indipendenti con poteri di indagine, di intervento e di avvio di azioni legali** (Art.1) e prevede il **divieto, in linea di principio, di trasferimento dei dati personali ad un paese che non offra la garanzia di un "livello adeguato di protezione"** (Art. 2). Il Protocollo Addizionale fu adottato soprattutto al fine di avvicinare il regime della Convenzione a quello della Direttiva sulla protezione dei dati dell'UE del 1995, di cui parleremo al punto 1.3, vedi *infra*.

Più di recente, nel maggio 2018, la Convenzione del 1981 venne ulteriormente "**aggiornata"**, per allinearla con la più recente legislazione sulla protezione dei dati dell'UE e, più in generale, con gli sviluppi (globali) riguardanti la protezione dei dati, come vedremo in seguito al punto 1.4.3.

In seno al Consiglio d'Europa, i problemi relativi alla protezione dei dati sono stati ulteriormente trattati da una serie di organismi, fra i quali l'Assemblea parlamentare del Consiglio d'Europa (PACE), il Comitato consultivo noto come "T-PD", creato ai sensi della Convenzione N°108 – responsabile del monitoraggio degli sviluppi in materia di protezione dei dati e dell'elaborazione di progetti settoriali, linee guida e raccomandazioni in materia - ed il Comitato dei Ministri del Consiglio d'Europa (COM o CM), incaricato dell'adozione di tali proposte. Questi organi hanno elaborato molti pareri, raccomandazioni e studi in materia, sempre facendo riferimento alla Convenzione.[53]

Inoltre, vi è interazione fra la Convenzione sulla protezione dei dati e la Convenzione europea sui diritti dell'uomo; la Corte europea dei diritti dell'uomo, infatti, si richiama sempre più alla Convenzione sulla protezione dei dati e agli strumenti giuridici summenzionati, nell'interpretazione dell'Articolo 8 della Convenzione dei diritti dell'uomo (che garantisce il diritto alla vita privata); l'Assemblea parlamentare (PACE), il Comitato consultivo e il Comitato dei Ministri, dal canto loro, si rifanno alla giurisprudenza della Corte in questo ambito.[54]

1.3 La legislazione comunitaria sulla protezione dei dati negli anni '90 e nei primi anni 2000

1.3.1 La protezione dei dati nella Comunità Europea

Contesto

---

[52] Si veda la nota 46, *supra*.

[53] Si veda:
http://website-pace.net/en_GB/web/apce/documents (documenti PACE). Sottolineiamo che questi documenti coprono molti altri ambiti che non la mera protezione dei dati, ma vanno ricercati alla voce "protezione dei dati".
https://www.coe.int/t/dghl/standardsetting/dataprotection/Documents_TPD_en.asp (documenti T-PD);
https://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp (documenti COM sulla protezione dei dati).

[54] Si veda la Scheda informativa – Protezione dei dati personali del Consiglio d'Europa (nota 13, *supra*) e l'*Allegato 1 – Giurisprudenza* al documento di lavoro del "Gruppo di lavoro Articolo 29" dell'UE, Documento di lavoro 01/2016 sulla giustificazione delle interferenze con i diritti fondamentali alla privacy e alla protezione dei dati attraverso misure di controllo nel trasferimento dei dati personali (Garanzie Essenziali Europee) (WP237), adottato il 13 aprile 2016, e contenente una lista di 15 importanti sentenze della CEDU sulla protezione dei dati (di cui cinque della CGUE):
http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf

Per un certo periodo, la Comunità Europea (la CEE, come veniva chiamata)[55] ritenne che la Convenzione sulla protezione dei dati personali del Consiglio d'Europa del 1981 garantisse, in questo campo, una tutela sufficiente. Alla fine del decennio, però, emerse chiaramente che la Convenzione non avrebbe portato ad una maggiore o più armonizzata protezione dei dati personali nella Comunità: al settembre del 1990, solo sette Stati membri della CEE l'avevano ratificata (di cui uno senza l'adozione della pertinente legislazione), e la legislazione di questi Stati divergeva in maniera considerevole su alcuni aspetti fondamentali.[56] All'epoca, l'Italia godeva solo di una legislazione sulla protezione dei dati riguardanti i lavoratori, la Spagna non aveva leggi omnibus, pur riconoscendo il diritto sancito dalla propria Costituzione alla protezione dei dati, ecc.

Questa frammentazione era inconciliabile con l'obiettivo della Comunità Europea dell'epoca di armonizzare tutte le leggi e le norme allo scopo di agevolare l'apertura del mercato interno con la realizzazione della libera circolazione di beni, servizi, capitali e persone. Più precisamente, in occasione della conferenza internazionale delle autorità di protezione dati del 1989, a Berlino, i rappresentanti lì riuniti furono informati dalla Commissione Europea che si sarebbe dovuto procedere ad un'armonizzazione delle norme riguardanti il settore delle telecomunicazioni. Una chiara dimostrazione della necessità che tutti gli Stati membri si dotassero di un forte sistema normativo in materia di protezione dei dati.[57]

L'anno seguente, nel settembre del 1990, in risposta a questo appello rivolto dalle autorità europee di protezione dati la Commissione Europea presentò una serie di proposte ambiziose e complesse finalizzate alla protezione dei dati personali in tutto il territorio della CE.[58] Il

---

[55] Al momento della presentazione del pacchetto di proposte della Commissione trattate in questa sezione (settembre 1990), la Commissione era ancora formalmente la "Commissione delle Comunità Europee" (al plurale). Il termine Comunità Europea (al singolare) venne utilizzato solo nel 1992, con il Trattato di Maastricht e fino all'entrata in vigore del Trattato di Lisbona nel 2009. Per maggior chiarezza faremo riferimento, in questa sezione, alla Comunità Europea e all'Unione Europea nella successiva sezione, la 1.4, e nella Seconda e Terza Parte.

[56] Commissione delle Comunità Europee, Comunicazione sulla protezione dei singoli in relazione al trattamento dei dati personali nella Comunità e alla sicurezza delle informazioni, COM(90) 314 finale – SYN287 e 288, Bruxelles, 13 settembre 1990, *Introduzione*. Il testo completo è disponibile online dall'ottimo archivio del Centre for Intellectual Property and Information Law dell'Università di Cambridge, all'indirizzo: https://resources.law.cam.ac.uk/cipil/travaux/data_protection/3%2013%20September%201990%20Communication.pdf.
Si vedano, in particolare, i paragrafi 6 – 8.

[57] Alla Conferenza internazionale delle Autorità di protezione dei dati svoltasi a Berlino nell'agosto del 1989, Spiros Simitis, Commissario alla protezione dei dati del Land Tedesco dell'Assia (e promulgatore della prima legge al mondo sulla protezione dei dati in questo Land), chiese pubblicamente a Jacques Fauvet, allora presidente dell'Autorità francese di protezione dei dati, la CNIL (ed ex-direttore del quotidiano "Le Monde"), di scrivere al suo vecchio amico Jacques Delors, Presidente della Commissione Europea, per chiedergli di intraprendere l'iniziativa di armonizzare la legislazione sulla protezione dei dati in seno alla CE.

[58] Il Trattato sull'Unione europea, firmato a Maastricht il 7 febbraio 1992 (il "Trattato di Maastricht") prevedeva una struttura a tre pilastri sorreggenti un unico frontone. Il Primo pilastro era costituito da quella che originariamente era la Comunità economica europea (CEE), dalla Comunità europea del carbone e dell'acciaio (CECA) e dalla Comunità europea dell'energia atomica (CEEA) (ognuna delle quali conservava comunque la rispettiva personalità giuridica), e successivamente venne a coincidere con il Mercato unico, creato nel 1993. Il Secondo e il Terzo pilastro riguardavano, rispettivamente, la politica estera e di sicurezza comune (PESC) e la cooperazione nei settori della giustizia e degli affari interni (GAI). I pilastri sono stati aboliti ufficialmente dal Trattato di Lisbona, ma tuttora gli strumenti giuridici emanati sono riferiti alle singole aree (v. l'analisi sull'ambito di applicazione del RGPD nella Parte II, paragrafo 2.3, *infra*). Si veda anche il sito web dell'Università del

pacchetto includeva proposte per due Direttive nell'ambito del Primo pilastro:[59]

- una **Direttiva generale della CE** (uno strumento giuridico limitato a quello che era il "Primo Pilastro" della Comunità Europea) "*relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali*" – che dopo un iter legislativo piuttosto lungo ha dato origine alla Direttiva sulla protezione dei dati della CE, la Direttiva 95/46/CE, di cui parleremo al punto 1.3.2; e
- un'ulteriore **Direttiva di carattere sussidiario** della CE "*sulla protezione dei dati personali nel contesto delle reti pubbliche di telecomunicazione digitale, in particolare nelle reti digitali di servizi integrati (ISDN) e nelle reti pubbliche digitali radiomobili*" – divenuta poi la Direttiva sulla protezione dei dati nel settore delle telecomunicazioni, Direttiva 97/66/CE, adottata nel dicembre 1997, e sostituita dalla Direttiva 2002/58/CE, la cosidetta Direttiva e-Privacy che analizzeremo al punto 1.3.3.

Prima di passare all'inqudramento di queste due Direttive è importante rilevare la natura e i limiti intrinseci di tali strumenti.

Lussemburgo su "Eventi storici nel processo di integrazione europea (1945-2014)", e in particolare la pagina dedicata a "Il Primo pilastro dell'Unione europea": https://www.cvce.eu/en/education/unit-content/-/unit/02bb76df-d066-4c08-a58a-d4686a3e68ff/4ee15c10-5bdf-43b1-9b5f-2553d5a41274. La direttiva del 1995 sulla protezione dei dati, e le altre direttive citate in questa sezione, sono state emanate in periodi ove ancora vigeva la suddivisione in pilastri, in particolare nell'ambito del Primo pilastro, e si riferivano esclusivamente a tale pilastro. Le disposizioni di protezione dati concernenti gli altri due pilastri sono descritte sinteticamente nei paragrafi 1.3.4 e 1.3.5, *infra*, mentre le norme di protezione dati applicabili alle istituzioni dell'Ue in quanto tali trovano spazio nel paragrafo 1.3.6.

[59] Commissione delle Comunità Europee, Comunicazione sulla protezione dei singoli in relazione al trattamento dei dati personali nella Comunità e alla sicurezza delle informazioni (nota precedente). Il pacchetto conteneva quattro ulteriori proposte:

- una bozza di **Risoluzione** dei rappresentanti degli Stati membri per l'estensione dell'applicazione dei principi contenuti nella Direttiva generale agli archivi in possesso delle autorità pubbliche ai quali la Direttiva principale sulla protezione dei dati personali non si sarebbe, in quanto tale, applicata. Il testo non fu mai adottato, ma può essere considerato la genesi della normativa sulla protezione dei dati in materia penale e giudiziaria, culminata, di recente, nella Direttiva relativa alla protezione dei dati da parte delle autorità competenti (Direttiva (EU) 2016/680 (non trattata in questo Manuale: si veda la nota al capitolo "*Il Manuale*" a pag. 1, *supra*);
- una bozza di **dichiarazione** della Commissione, relativa all'applicazione degli standard sulla protezione dei dati fissati dalla Direttiva sulla protezione dei dati agli archivi in possesso delle stesse istituzioni della Comunità – testo che poi ha portato al Regolamento (EC) 45/2001 (*idem*);
- una **Raccomandazione per decisione del Consiglio** sull'adesione alla Convenzione sulla protezione dei dati del Consiglio d'Europa da parte della Comunità Europea – di cui all'epoca non si fece nulla perché la UE, non essendo uno Stato membro, non poteva aderire alla Convenzione; il problema è stato risolto nella Convenzione "aggiornata" sulla protezione dei dati del Consiglio d'Europa, di cui parleremo al punto 1.4.3; e
- una **proposta per decisione del Consiglio** sull'adozione di un piano d'azione sulla sicurezza delle informazioni – che generò un'intensa attività in materia da parte dell'UE, tra cui la creazione, nel 2004, dell'ENISA, l'Agenzia Europea per la sicurezza delle reti e dell'informazione, e l'elaborazione di un'elaborata strategia sulle informazioni e la sicurezza informatica, che non affronteremo in questo Manuale, ma sulla quale si possono trovare utili informazioni su:
  https://www.enisa.europa.eu/about-enisa
  https://ec.europa.eu/digital-single-market/en/cyber-security

Per le proposte che figurano nella lista della Comunicazione della Commissione (e altri documenti relativi al processo legislativo) si vedano i link di questa pagina:
https://www.cipil.law.cam.ac.uk/projectseuropean-travaux/data-protection-directive

Natura e limiti delle Direttive CE

Nella discussione riguardante i principali strumenti della protezione dei dati nell'UE, e in particolare le due Direttive sulla protezione dei dati poc'anzi citate, vanno tenuti a mente tre elementi. Prima di tutto, ogni strumento giuridico dell'UE (in passato CE) è, per sua natura, limitato alle materie di competenza del diritto dell'UE (in passato CE). Alcune materie, soprattutto le attività degli Stati membri nell'ambito della **sicurezza nazionale**, non rientrano affatto (con poche eccezioni) tra le competenze giuridiche dell'UE (in passato CE),[60] e nessuno strumento normativo dell'UE (o CE), comprese le Direttive di cui sopra, il RGPD o qualunque futura norma sulla protezione dei dati dell'UE, sotto qualsiasi forma, potrà essere di applicazione in questi ambiti. Il concetto è stato espressamente ribadito nelle Direttive (e nel RGPD): si veda l'Art. 3(2) della Direttiva sulla protezione dei dati del 1995 e l'Art. 1(3) della Direttiva e-Privacy (nonché l'Art.2(2)(a) del RGPD).[61]

Inoltre, le Direttive CE di cui parleremo si limitavano, in quanto tali, a materie nell'ambito del cosiddetto **Primo Pilastro**[62], e per la loro natura di Direttive CE non si applicavano alle attività del Secondo o Terzo Pilastro, per i quali sono stati elaborati a parte degli strumenti di protezione dei dati personali che sono descritti sinteticamente nei paragrafi 1.3.4 e 1.3.5, ma non rientrano nell'ambito di trattazione del presente volume. È sufficiente notare che *qualunque cessione di dati o messa a disposizione di dati personali* da parte di istanze regolamentate dalle Direttive (sia del settore privato che pubblico e operanti nell'ambito della legislazione (CE) del "Primo Pilastro") alle forze dell'ordine o ad organismi di sicurezza nazionale era (e nel caso della direttiva e-Privacy, ancora è) disciplinata da tali strumenti (poiché tali divulgazioni, ai sensi delle direttive, costituiscono "trattamento" da parte di queste istanze), mentre l'*ottenimento (ricezione) e l'ulteriore trattamento* dei dati divulgati erano regolamentati da altri strumenti (compresi, fino a poco tempo fa, la Decisione quadro del Consiglio 2008/977/CGUE, soprattutto nella parte che riguarda le forze dell'ordine e, più di recente, la Direttiva sulla protezione dei dati nelle attività di contrasto del 2016), o non affatto subordinati al diritto comunitario (ad es., se tale ottenimento e trattamento fosse operato da organismi di sicurezza nazionale).[63]

Terzo, una direttiva, per definizione, non si applica direttamente agli ordinamenti giuridici degli Stati membri e non ha un "effetto diretto". Le sue disposizioni devono essere "**recepite**", piuttosto, negli ordinamenti nazionali degli Stati membri – che in questo godono (ed hanno

---

60 Diciamo "(quasi) del tutto" per due motivi. Primo, perché è diventato sempre più difficile, soprattutto in relazione al terrorismo (in sé un concetto non meglio precisato) operare un distinguo fra le azioni dello Stato in materia di sicurezza nazionale e quelle nell'ambito del diritto penale o del diritto finalizzato alla tutela della "sicurezza internazionale", "sicurezza pubblica" o "ordine pubblico" – tutti ambiti che sono oggi, in misura maggiore o minore, di competenza almeno parziale del diritto dell'UE. Secondo, anche se le azioni intraprese dagli organismi degli Stati membri incaricati della sicurezza nazionale, si situano al di fuori del campo di applicazione del diritto comunitario, operazioni strettamente connesse da parte delle forze dell'ordine o di entità private (ad es. la raccolta e la divulgazione dei dati bancari sottoposti a norme di antireciclaggio, o la raccolta e la divulgazione dei dati delle liste passeggeri delle linee aeree ad agenzie degli Stati membri) rientrano spesso nell'ambito di applicazione del diritto comunitario (in particolare le norme di tutela dei dati personali). Cfr. il secondo punto del testo.

61 Sulle limitazioni dell'ambito di applicazione del Regolamento sulla protezione dei dati dell'UE si veda le Seconda Parte, sezione 2.3, *Elementi chiave del RGPD*, in particolare la sotto sezione 2.3.1, Disposizioni generali.

62 V. nota 67, *infra*.

63 Su questioni simile emerse in relazione al Regolamento dell'UE sulla protezione generale dei dati si rimanda alla Seconda Parte, in particolare alla sezione 2.2, *Natura giuridica e approccio del RGPD: armonizzazione e flessibilità*.

goduto in passato) di un notevole potere di **discrezionalità**. Così è stato per le due Direttive che analizzeremo fra poco e questo ha generato, come evidenziato nella Seconda Parte, notevoli divergenze fra gli ordinamenti giuridici degli Stati membri che le hanno recepite. Questo è stato uno dei motivi principali che hanno determinato la scelta di un Regolamento (direttamente applicabile) quale sostituto della Direttiva sulla protezione dei dati del 1995, il RGPD (benché, come avremo modo di sottolineare in questa parte, anche un Regolamento possa essere attuato in modi diversi e con diversi aspetti).[64]

1.3.2 La Direttiva CE sulla protezione dei dati del 1995

Quadro generale

Come già rilevato, all'inizio degli anni '90, la Commissione delle Comunità Europee (secondo la denominazione dell'epoca)[65] si trovava di fronte a un dilemma: da un lato, la protezione dei dati era sempre più riconosciuta come un diritto protetto costituzionalmente nell'UE, e questo imponeva restrizioni nell'utilizzo e nello scambio dei dati;[66] dall'altro, lo sviluppo del **mercato interno**, nel cosidetto "Primo Pilastro" della Comunità,[67] imponeva il libero scambio dei dati, compresi i dati personali, inerenti alle transazioni commerciali. Per far quadrare il

---

[64] Si veda la Seconda Parte, sezione 2.2, *Natura giuridica e approccio del RGPD: armonizzazione e flessibilità*.

[65] Si veda la nota 67, *infra*.

[66] La protezione dei dati è oggi chiaramente riconosciuta come un diritto *sui generis* all'Articolo 8 della Carta dei Diritti fondamentali dell'UE (CDFUE), diritto distinto (anche se in stretta relazione) da quello alla vita privata e familiare e dal diritto alla privacy, la cui tutela è garantita all'Articolo 7. La CDFUE risale al 2000, ma non ha avuto piena validità giuridica fino all'entrata in vigore del Trattato di Lisbona il 1°dicembre 2009. Si veda: https://en.wikipedia.org/wiki/Charter_of_Fundamental_Rights_of_the_European_Union
In altri termini, la Carta non aveva ancora piena validità giuridica all'epoca in cui le due Direttive vennero proposte. Comunque, anche prima che la Carta fosse redatta o avesse piena validità giuridica, i diritti fondamentali godevano di una valenza quasi costituzionale nelle Comunità Europee, si veda: Francesca Ferraro e Jesús Carmona, I Diritti fondamentali nell'Unione Europea – Il ruolo della Carta dopo il Trattato di Lisbona Servizio ricerche del Parlamento, Bruxelles, marzo 2015, sezione 2*: EU Fundamental rights prior to the Lisbon Treaty*, disponibile alla pagina:
http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/554168/EPRS_IDA(2015)554168_EN.pdf
I redattori della Direttiva sulla protezione dei dati del 1995 individuarono, a giusto titolo, nella protezione dei dati personali il fondamento di questo strumento legislativo.

[67] Il Trattato dell'Unione Europea, firmato a Maastricht il 7 febbraio 1992 (il "Trattato di Maastricht"), prevedeva una struttura a tre pilastri sotto un unico frontone. Il Primo Pilastro era costituito dalle originarie Comunità Economica Europea (CEE), Comunità Europea del carbone e dell'Acciaio (CECA) e Comunità Europea dell'Energia Atomica (EURATOM) (sebbene ciascuna conservasse la propria personalità giuridica). Il Secondo ed il Terzo Pilastro coprivano, rispettivamente, la Politica estera e di sicurezza comune (PESC) e la cooperazione nell'ambito della Giustizia e degli Affari interni (GAI). I Pilastri furono ufficialmente aboliti con il Trattato di Lisbona, ma i vari ambiti sono ancora coperti da vari strumenti (cfr. la discussione sul campo di applicazione del RGPD nella Seconda Parte, sezione 2.3, *infra*). Si consulti anche il sito web del Centro di ricerca CVCE dell'Università del Lussemburgo sugli Eventi storici nel processo di integrazione europea (1945 – 2014), in particolare la pagina riguardante "*Il Primo Pilastro dell'Unione Europea*":
https://www.cvce.eu/en/education/unit-content/-/unit/02bb76df-d066-4c08-a58a-d4686a3e68ff/4ee15c10-5bdf-43b1-9b5f-2553d5a41274
Si veda anche la voce "I tre pilastri dell'Unione europea" su Wikipedia, consultabile qui: https://en.wikipedia.org/wiki/Three_pillars_of_the_European_Union (con un utilissimo grafico della successione cronologica).
La Direttiva sulla protezione dei dati del 1995 (e le altre trattate nella presente sezione) era (ed erano) state elaborate all'epoca dell'esistenza del Primo Pilastro ed erano finalizzate solo a questo pilastro.

cerchio, la Commissione propose, per il "Primo Pilastro" l'adozione di due Direttive. In questa sede affronteremo la più importante delle due, la Direttiva 95/46/CE.[68]

Scopi e finalità della Direttiva sulla protezione dei dati del 1995

Riconoscendo il dilemma di cui dicevamo, la Commissione Europea individuò per la Direttiva due finalità correlate: garantire un **elevato livello di protezione dei dati,** valido per tutto il "Primo Pilastro" della Comunità ("elevato livello" perché la direttiva mirava a tutelare diritti umani) e quale *conditio sine qua non* per la **libera circolazione dei dati personali** all'interno della componente principale di questo pilastro, **il mercato interno** allora emergente (si veda l'Articolo 1 della Direttiva, il Considerando 10 e, soprattutto, 11).

Elementi essenziali della Direttiva sulla protezione dei dati del 1995

Gli **elementi essenziali** della Direttiva sulla protezione dei dati del 1995 rispetto alla Convenzione del 1981 (NB: gli elementi nuovi o contenenti importanti elementi di novità sono contrassegnati con la dicitura *NUOVO) sono indicati nel prosieguo. Si tenga presente, tuttavia, che spesso tali elementi si fondano sulle componenti già indicate in modo più o meno esplicito nei "considerando" della Convenzione. Se ne fornisce una descrizione sintetica in questa sede per offrire un quadro sinottico di alcuni elementi costitutivi dell'approccio alla protezione dei dati nell'Ue, i quali hanno trovano piena conferma nel Regolamento generale del 2016; viceversa, i principali elementi di novità contenuti nel suddetto Regolamento saranno oggetto di trattazione nella Parte II. Le principali novità riguardavano la creazione su base obbligatoria di autorità indipendenti per la protezione dei dati e le misure previste per garantire la tutela dei dati anche ove trasferiti verso Paesi terzi (ossia, al di fuori dell'Ue/del SEE).

*NUOVO Definizioni

La Direttiva ha ampliato le **definizioni di base** della Convenzione del 1981 aggiungendone di nuove. Nello specifico, ha chiarito (all'interno della definizione di "dati personali") quando una persona fisica possa essere "***identificabile***" (rispetto al concetto di "chiunque"), e (in una definizione separata) quando un insieme di dati inseriti manualmente possano essere considerati come sufficientemente "***strutturati***" da rientrare nell'applicazione della Direttiva. "I casellari manuali [strutturati]" sono stati inclusi nell'ambito della Direttiva per evitare l'elusione delle norme nell'utilizzo degli stessi.

La Direttiva fissa una ***definizione leggermente modificata di "titolare del trattamento"***, aggiunge ***una nuova definizione globale di "trattamento di dati personali"*** e definisce concetti quali "***responsabile del trattamento***", "***terzi***" e "***destinatario***". Aggiunge, inoltre, una definizione di "***consenso della persona interessata***" e le condizioni che devono essere riunite perchè un consenso al trattamento sia considerato valido: il consenso, per essere ritenuto valido, deve essere una "***manifestazione di volontà libera, specifica e informata"***, e, in un certo modo, ***espressa*** (Art. 2(h)).[69]

Mentre la Convenzione del 1981 aveva quattro definizioni, la Direttiva ne conteneva otto (o

[68] Titolo completo: Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati , GU L281, 23.11.1995, pp. 31 – 50, disponibile all'indirizzo: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN

[69] Il consenso deve prendere la forma di una "**manifestazione di volontà** libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento", per citare il testo.

nove, se si conta anche la definizione di "persona identificabile o identificata" all'interno della definizione di "dati personali").

Principi di Protezione dei dati

La Direttiva riprendeva ampiamente i **principi della protezione dei dati** della Convenzione del 1981, ma con alcuni **chiarimenti**, fra cui lo ***scopo*** per il quale i dati personali devono essere trattati, il quale deve essere non solo "*specificato*" e "*legittimo*" (come stabilito dall'Art. 5(b) della Convenzione), ma anche "*esplicito*" (Art. 6(1)(b)), nonché con riguardo ai *"trattamenti ulteriori per scopi storici, statistici o scientifici"* (Art. 6(1)(c) e (e)).

**NUOVO Base giuridica per il trattamento dei dati

Una grande novità della Direttiva del 1995, introdotta al fine di garantire una maggiore armonizzazione della legislazione degli Stati membri, fu l'individuazione di una serie di principi, di cui all'Articolo 7, e più esattamente di una **lista esaustiva di "principi relativi alla legittimazione del trattamento dei dati"** – che in seguito sarebbero stati definiti le **"basi giuridiche" per il trattamento dei dati personali**. Riassumendo, ai sensi della Direttiva, il trattamento dei dati personali (non sensibili) poteva essere effettuato solo quando:

(a) la persona interessata ha manifestato il proprio **consenso in maniera inequivocabile**, (consenso che deve naturalmente essere "**manifestazione di libera volontà, specifica, informata**" e "**espressa"**, Art. 2(h), di cui abbiamo già parlato); oppure

(b) il trattamento **è necessario** all'esecuzione del **contratto** concluso con la persona interessata o all'esecuzione di misure precontrattuali prese su richiesta di tale persona (ad es., per una verifica di solvibilità); oppure

(c) il trattamento è **necessario** per adempiere **un obbligo legale** al quale è soggetto il responsabile del trattamento; oppure

(d) il trattamento **è necessario** per la salvaguardia dell'**interesse vitale della persona interessata**; oppure

(e) il trattamento è **necessario** per lo svolgimento di **un compito di interesse pubblico o nell'esercizio di pubblici poteri** di cui è investito il responsabile del trattamento o il terzo cui vengono comunicati i dati; oppure

(f) il trattamento è **necessario** per il perseguimento **dell'interesse legittimo** del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata, che richiedono tutela ai sensi dell'Articolo 1(1). [il cosidetto "interesse legittimo" o criterio/base giuridica del"bilanciamento"].

In sostanza, nella maggioranza dei casi era consentito trattare dati personali non sensibili sulla base di una norma di legge o per fini contrattuali, oppure con il consenso della persona interessata, o per il perseguimento di un interesse legittimo del titolare purché non prevalessero gli interessi o i diritti e le libertà fondamentali della persona interessata.

Questa lista non figurava nella Convenzione sulla protezione dei dati del 1981.

** *NUOVO Regole specifiche per i trattamenti dei dati sensibili

La Direttiva del 1995 elenca anche le **principali** "**categorie particolari di dati**" – che comunemente si definiscono come "**dati sensibili**" – in gran parte corrispondenti a quelle già

fissate dalla Convenzione del 1981, con alcune modifiche minori, ad es.:[70]

> i dati a carattere personale che rivelano l'origine raziale o *etnica*, le opinioni politiche, le convinzioni religiose o *filosofiche*, *l'appartenenza sindacale*, nonché … i dati relativi alla salute e alla vita sessuale…

Non volendo limitarsi ad affermare che questi dati "*non possono essere elaborati automaticamente a meno che il diritto nazionale non preveda delle garanzie appropriate*" (Convenzione del Consiglio d'Europa, Art. 6), la Direttiva, all'Articolo 8(1), sancisce **il divieto, in linea di principio,** al trattamento di questi dati sensibili, con un numero limitato di **eccezioni**. Le eccezioni principali, in effetti, si riferiscono **a basi giuridiche particolarmente restrittive** per il trattamento dei dati sensibili. Riassumendo, possiamo dire che il divieto di trattamento non si applica qualora:

- la persona interessata abbia dato il proprio **consenso non solo libero, specifico e informato, ma anche *esplicito*** a tale trattamento, salvo nei casi in cui la legislazione dello Stato membro preveda che il consenso della persona interessata non sia sufficiente per derogare al divieto di cui al paragrafo 1 (art. 8(2)(a));
- il trattamento sia ***necessario***, per assolvere gli obblighi e i diritti specifici del titolare del trattamento in materia di **diritto del lavoro**, nella misura in cui il trattamento stesso sia autorizzato da norme nazionali che prevedono adeguate garanzie (Art. 8(2)(b));
- il trattamento sia ***necessario*** per salvaguardare un **interesse vitale** della persona interessata o di un terzo nel caso in cui la persona interessata sia nell'incapacità fisica o giuridica di dare il proprio consenso (Art. 8(2)(c));
- il trattamento "sia effettuato, con garanzie adeguate, da una fondazione, un'associazione o qualsiasi altro **organismo che non persegua scopi di lucro e rivesta carattere politico, filosofico, religioso o sindacale**, nell'ambito del suo scopo lecito e a condizione che riguardi unicamente i suoi ***membri*** o le ***persone che abbiano contatti regolari*** con la fondazione, l'associazione o l'organismo a motivo del suo oggetto e che i dati ***non vengano comunicati a terzi*** senza il consenso della persona interessata" (Art. 8(2)(d));
- il trattamento riguardi dati (sensibili) "**resi manifestamente pubblici dalla persona interessata**" (Art. 8(2)(e), prima parte dell'enunciato); e
- il trattamento riguardi dati (sensibili) necessari per costituire, esercitare o difendere un diritto per **via giudiziaria**" (Art. 8(2)(e), seconda parte dell'enunciato).

Bisogna osservare che la lista non includeva un criterio di "**legittimo interesse**" o di "**bilanciamento**": i dati sensibili non potevano essere trattati *in linea di principio*, già ai sensi della Direttiva, nel legittimo interesse del titolare del trattamento o di terzi, anche qualora non prevalessero i diritti fondamentali della persona interessata.

La Direttiva prevedeva comunque che il divieto, in linea di principio, di trattamento dei dati sensibili (nota: di ogni tipo di dato sensibile) non fosse di applicazione quando "*il trattamento dei dati è **necessario** alla **prevenzione o alla diagnostica medica,** alla **somministrazione** di **cure** o alla **gestione di centri di cura**",* a patto che il trattamento dei medesimi dati venisse effettuato da un professionista soggetto al segreto professionale o ad un obbligo equivalente (Art. 8(3)). Rileviamo che la norma è di applicazione per tutti i dati sensibili – naturalmente

[70] La Convenzione del 1981 non faceva riferimento a dati "etnici", ma parlava "di convinzioni religiose o altre convinzioni" (piuttosto che di "convinzioni religiose o filosofiche"), e non includeva l'appartenenza sindacale.

con il vincolo che tali dati vengano utilizzati per le finalità evocate nel rispetto della normativa (ad es, le informazioni relative all'origine etnica possono essere importanti nel quadro di certe patologie come l'anemia falciforme, oppure il credo religioso di una persona può essere importante in alcuni trattamenti, pensiamo alle trasfusioni di sangue per i Testimoni di Geova).

Sebbene queste norme siano, di per sé, rigorose, la Direttiva conteneva anche una clausola espressa in termini più ampi che prevedeva che gli Stati membri potessero stabilire **ulteriori deroghe** (Art. 8(4)) – cioè permettere il trattamento di (qualunque tipo di) dati sensibili diversi da quelli di cui all'Articolo 8(2) – sulla base della legislazione nazionale o di una decisione dell'autorità di controllo (autorità della protezione dei dati), "***per motivi di interesse pubblico rilevante***", a condizione che fossero previste le "***opportune garanzie***" – definite dagli Stati membri.

La Direttiva fissava anche norme più restrittive al trattamento dei **dati personali relativi alle infrazioni, alle condanne penali o alle misure di sicurezza** (Art. 8(5)) e ai **numeri nazionali di identificazione o qualsiasi altro "mezzo identificativo di portata generale"** (Art. 8(7)), pur lasciando la regolamentazione dei dettagli del trattamento agli Stati membri.

Allo stesso modo, benché la Direttiva, rispetto alla Convenzione del 1981, enfatizzasse maggiormente la necessità di un **equilibrio fra la protezione dei dati e la libertà di espressione e di informazione,** lasciava poi la ricerca di questo equilibrio anche all'azione legislativa degli Stati membri (Art. 9).

*NUOVO Informazione della persona interessata

La Convenzione sulla protezione dei dati del 1981 imponeva solo una generica trasparenza sulla possibilità che ciascuno avesse "*di conoscere l'esistenza di una raccolta automatizzata di dati, i suoi fini principali, nonché l'identità e la residenza abituale o la sede principale del titolare della raccolta dei dati*" (Art. 8(a)).

Gli Articoli 10 e 11 della Direttiva sulla protezione dei dati del 1995, invece, definiscono in modo dettagliato ***le informazioni che il titolare del trattamento deve fornire alla persona interessata***, *le finalità del trattamento da parte del titolare*, quando i dati siano raccolti presso la persona interessata o da terzi. In entrambi i casi, è obbligatorio fornire ***l'identità del titolare del trattamento*** e le ***finalità del trattamento***. ***Ulteriori informazioni*** (comprese quelle riguardanti l'obbligatorietà o meno della raccolta dei dati e le informazioni sul qualunque tipo di divulgazione dei dati) devono essere fornite qualora siano necessarie per effettuare un trattamento leale (si vedano gli Art.10(c) e 11(1)(c)).

*NUOVO I diritti della persona interessata

Già la Convenzione sulla protezione dei Dati personali del 1981 garantiva che le persone interessate godessero: del diritto di **accesso** ai loro dati, su richiesta e ad intervalli ragionevoli di tempo; del diritto di **rettifica o cancellazione** dei dati inesatti o trattati in violazione delle norme sulla protezione dei dati e del diritto di **ricorso** se l'esercizio di questi diritti non fosse stato rispettato (Art. 8(b) – (d)).

La Direttiva ha confermato i primi due diritti, con **un ulteriore dettaglio importante**. Ha infatti confermato che il **diritto di accesso** include il diritto di "comunicazione" dei dati alla persona interessata (come già sancito nella Convenzione), aggiungendo però che tale comunicazione debba avvenire "*in forma comprensibile*" e si garantiscano "*tutte le informazioni disponibili sull'"**origine"** dei dati* (Art. 12(a), secondo paragrafo). Il "***blocco***" viene aggiunto quale opzione

alla rettifica e alla cancellazione (senza peraltro definirne il concetto)[71] (Art. 12(b)); e si garantisce che qualsiasi rettifica, cancellazione o congelamento debbano essere notificati ai ***terzi*** cui i dati sono stati comunicati (Art. 12(c)).

La Direttiva ha individuato anche nuovi diritti: un **diritto generale di opposizione** al trattamento per "motivi preminenti e legittimi", "almeno" per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, o basato sul criterio dell'"interesse legittimo"/"equilibrio" – un diritto di opposizione riconosciuto qualora "giustificato" (Art. 14(a)); **un diritto** più dettagliato e più forte **di opporsi al trattamento dei dati personali a fini di invio di materiale pubblicitario** (all'epoca effettuato soprattutto via posta, prima dell'era di Internet e degli invii "spam") – che doveva essere sempre rispettato, senza che la persona interessata dovesse giustificarsene (Art. 14(b)); e il **diritto, per la persona interessata, di non essere sottoposta a valutazione di aspetti della personalità che si fondi esclusivamente su un trattamento automatizzato di dati**[72] e che produca effetti giuridici o significativi (con una serie di importanti e ben definite ***deroghe***) (Art. 15). A tal proposito, va rilevato che l'Articolo 12(a), terzo capoverso, sancisce che le persone interessate dispongono del **nuovo** diritto di ottenere (in caso di richiesta di accesso ai dati,) **informazioni sulla "logica"** applicata nei trattamenti automatizzati dei dati che li riguardano, "quanto meno" nel caso di valutazione di aspetti della personalità che si fondi esclusivamente su un trattamento automatizzato.

Questi diritti come già fissati nella direttiva del 1995, e confermati e ulteriormente rafforzati nel RGPD, acquistano ancora maggiore rilievo guardando ai processi decisionali fondati sull'intelligenza artificiale.

*NUOVO Riservatezza e sicurezza dei trattamenti

La Convenzione del 1981 prevedeva semplicemente che si dovessero prendere "idonee misure di sicurezza" per proteggere i dati personali contro "la distruzione accidentale o non autorizzata o la perdita accidentale, nonché contro l'accesso, la modifica o la diffusione non autorizzati" (Art. 7).

La Direttiva ha ampiamente approfondito questi aspetti imponendo, prima di tutto, un **dovere di riservatezza** a chiunque sia coinvolto nel trattamento dei dati personali (Art. 16), e inoltre sancendo che il titolare del trattamento debba adottare "*misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali*" (Art. 17(1), che contiene anche altri dettagli). Questa norma è stata ripresa dalla Legge federale tedesca sulla protezione dei dati del 1977.

Si stabiliscono, inoltre, nuovi importanti obblighi nel caso in cui il titolare del trattamento scelga un responsabile per eseguire un trattamento per proprio conto: il responsabile deve presentare "*garanzie sufficienti*" a livello della sicurezza e della riservatezza. Si sancisce,

---

[71] Il concetto corrispondente della "**limitazione di trattamento**" è definito nel RGPD come "*il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro*" (Art. 4(3) RGPD).

[72] Testo completo: "*Gli Stati membri riconoscono a qualsiasi persona il diritto di non essere sottoposta ad una decisione che produca effetti giuridici o abbia effetti significativi nei suoi confronti fondata esclusivamente su un trattamento automatizzato di dati destinati a valutare taluni aspetti della sua personalità, quali il rendimento professionale, il credito, l'affidabilità, il comportamento, ecc*". La norma è stata direttamente mutuata dalla Legge francese sulla protezione dei dati del 1978, Articoli 2 e 3.

inoltre, che gli elementi del contratto per la protezione dei dati fra il titolare del trattamento e il responsabile del trattamento siano stipulati per iscritto (Art. 17(2) – (4)).

*NUOVO Restrizioni ai trasferimenti di dati verso un paese terzo

Come osservato al punto 1.2.3, la Convenzione del 1981, nel suo testo originale, non chiedeva agli Stati firmatari di adottare **il divieto di esportazione dei dati personali dal proprio territorio a quello di uno Stato che non garantisse tutele assimilabili,** disciplinando soltanto i flussi di dati personali fra i firmatari della Convenzione. L'introduzione di questo divieto (con una serie di eccezioni limitate), derivante dall'esperienza legislativa francese e danese, è stata un'altra importante novità della Direttiva del 1995.

Nello specifico, la Direttiva prevede che i dati personali che rientrano nel suo ambito applicativo possano essere trasferiti verso un paese terzo solo nel caso in cui questi garantisca un livello di protezione "**adeguato**" ai sensi della Direttiva (Art. 25(1)); e che la Commissione Europea abbia facoltà di constatare e decidere (con quella che venne denominata "**decisione di adeguatezza**") l'adeguatezza del livello di protezione dei dati di un determinato paese terzo (Art. 25(2)).[73] La Commissione stabilì il concetto di "adeguatezza" non solo in relazione ai paesi terzi nel loro congiunto, ma anche a **settori** in specifici paesi (per es, all'inizio, il regime degli organismi del settore pubblico in Canada) e perfino a **programmi** particolari adottati in determinati paesi (come, ad. es, il regime di "*Safe Harbor*" degli USA, poi sostituito dal regime di "*Privacy Shield*").

Il divieto, in linea di principio, di trasferire dati a paesi (o a settori di determinati paesi) senza protezione adeguata, veniva derogato con un certo numero di **eccezioni** che figurano all'Articolo 26(1) della Direttiva, molte delle quali simili alle basi giuridiche per il trattamento in generale. In breve, possiamo dire che è necessario che:

(a) la persona interessata abbia manifestato il proprio **consenso** al trasferimento in ***maniera inequivocabile*** (consenso che, naturalmente, deve essere"***libero, specifico e informato***" e ***espresso***: Art. 2(h), come in precedenza rilevato);

(b) il trasferimento sia ***necessario*** per l'esecuzione di un **contratto** tra la persona interessata ed il titolare del trattamento o per l'esecuzione di misure precontrattuali su richiesta della persona interessata (ad es., per una verifica di solvibilità);

(c) il trasferimento sia ***necessario*** per la conclusione o l'esecuzione di un **contratto**, concluso o da concludere nell'interesse della persona interessata, tra il titolare del trattamento e un terzo (per es., la prenotazione di un hotel);

(d) il trasferimento sia ***necessario*** o ***prescritto dalla legge*** per la salvaguardia di un interesse pubblico rilevante, oppure per costatare, esercitare o difendere un diritto ***per via giudiziaria***;

(e) il trasferimento sia ***necessario*** per la salvaguardia ***dell'interesse vitale della persona interessata***;

(f) il trasferimento avvenga a partire da un **registro pubblico** (subordinato alle condizioni di accesso ai registri in generale).

---

[73] Il termine "protezione adeguata" venne scelto perchè il termine "equivalente" era riservato, nel diritto comunitario, ai rapporti normativi fra Stati membri, mentre, alla luce del diritto internazionale, il termine avrebbe dovuto significare "di effetto equivalente". Nella sentenza *Maximillian Schrems contro il Commissario alla protezione dei dati*, Sentenza CGUE nel procedimento C-362/14, del 6 dicembre 2015, la Corte ha stabilito che il termine "protezione adeguata" debba essere interpretato come protezione "sostanzialmente equivalente" nello Stato terzo: si veda il par. 96 della sentenza – intervenuta molti anni dopo l'adozione della Direttiva del 1995 (o del Protocollo addizionale del 2001 alla Convenzione del 1981, come avremo modo di notare).

Inoltre, gli Stati membri possono **autorizzare** trasferimenti qualora il titolare del trattamento presti "***garanzie sufficienti***" per la tutela della vita privata e dei diritti e delle libertà fondamentali degli interessati (Art. 26(2)) – ad es., sotto forma di ***clausole ad hoc per il trasferimento dei dati ;*** la Commissione è stata **autorizzata** ad approvare alcune "***clausole contrattuali standard***" per il trasferimento dei dati, in grado di garantire tale tutela (Art. 26(4)).

Molte Autorità di protezione dati, seguite dal WP29, presero in considerazione anche le garanzie contenute nelle cosiddette ***norme vincolanti d'impresa*** **(BCR)**, ossia in regole fissate da società o gruppi societari internazionali con cui si disciplinavano gli utilizzi e i flussi intra-gruppo di dati personali.[74] Nonostante le esitazioni mostrate da alcune Autorità, questo strumento ha poi trovato accoglimento all'interno del RGPD (v. Parte II).

Le limitazioni poste ai trasferimenti di dati personali verso Paesi terzi in assenza di tutele adeguate stimolarono varie iniziative al di fuori dell'Europa. In particolare, le Autorità di protezione dati francesi e spagnole se ne servirono per promuovere l'adozione di una normativa adeguata nelle aree geografiche omologhe linguisticamente – cioè nell'America latina e nei Paesi francofoni soprattutto africani.

NB: come sottolineato al punto 1.2.3, *supra*, una norma di "adeguatezza" per il trasferimento dei dati fu introdotta nella Convenzione del 1981 dal Protocollo Aggiuntivo alla Convenzione del 2001, allo scopo di allineare il regime della Convenzione a quello della Direttiva CE del 1995 (si veda l'Art. 2(1) del Protocollo) – sebbene questa norma fosse di applicazione solo agli Stati firmatari sia della Convenzione del 1981 che del Protocollo.[75]

*NUOVO Codici di condotta (e certificazioni)

Un'altra novità introdotta dalla Direttiva è stato il riferimento a **codici di condotta** quali mezzi per "*contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle*

[74] Le BCR sono oggetto di numerosi documenti di lavoro e raccomandazioni elaborati dal WP29, fra cui i seguenti:

- Documento di lavoro: Trasferimenti di dati personali verso Paesi terzi: Applicazione dell'art. 26(2) della direttiva UE sulla protezione dei dati a norme vincolanti d'impresa per i trasferimenti internazionali di dati, adottato dal Gruppo di lavoro "Articolo 29" il 3 giugno 2003 (WP74);
- Documento di lavoro che definisce un modello di checklist per la richiesta di approvazione di norme vincolanti d'impresa, adottato dal Gruppo di lavoro "Articolo 29" il 3 giugno 2003 (WP108);
- Raccomandazione 1/2007 sulla richiesta standard di approvazione di norme vincolanti d'impresa per il trasferimento di dati personali, adottata dal Gruppo di lavoro "Articolo 29" il 10 gennaio 2007 (WP133);
- Docoumento di lavoro che istituisce una tabella degli elementi e dei principi che devono figurare nelle norme vincolanti d'impresa, adottato dal Gruppo di lavoro "Articolo 29" il 24 giugno 2008 (WP153);
- Documento di lavoro che istituisce una cornice strutturale per le norme vincolanti d'impresa, adottato dal Gruppo di lavoro "Articolo 29" il 24 giugno 2008 (WP154);
- Documento di lavoro sulle domande più frequenti (FAQ) relative alle norme vincolanti d'impresa, adottato dal Gruppo di lavoro "Articolo 29" il 24 giugno 2008, come rivisto e adottato l'8 aprile 2009 (WP155);
- Documento di lavoro 2/2012 che istituisce una tabella degli elementi e dei principi che devono figurare nelle norme vincolanti d'impresa per responsabili del trattamento, adottato il 6 giugno 2012 (WP195).

Si veda anche:

- Parere 02/2014 relativo a un repertorio dei requisiti relativi alle norme vincolanti d'impresa presentate alle autorità nazionali per la protezione dei dati nell'Ue e alle norme transfrontaliere in materia di privacy presentate agli agenti responsabili delle CBPR dei paesi dell'APEC, adottato il 27 febbraio 2014 (WP212).

[75] Si veda la nota 46, *supra*. Si osservi che non è chiaro se il termine "adeguato" nel suddetto articolo del Protocollo debba o possa essere interpretato conformemente alla sentenza nel caso Schrems (v. nota 73, *supra*), e quindi se il Protocollo stesso abbia conseguito l'obiettivo che si era prefisso.

disposizioni nazionali di attuazione della presente direttiva, adottate dagli Stati membri" (art. 27(1)) – benché la Direttiva si limiti ad "incoraggiare" tali codici (*idem*), chiedere che gli Stati membri adottino norme per la valutazione di ***progetti di codici nazionali*** (Art. 27(2)) e che gli Stati provvedano a che ***progetti di codici comunitari*** possano essere sottoposti, per valutazione, al Gruppo di Lavoro Articolo 29 (WP29, di cui parleremo in questo stesso capitolo), (Art. 27(3)).

Nella pratica, solo un numero molto limitato di questi codici è arrivato all'approvazione o anche solo alla fase di presentazione per l'approvazione. La prima bozza del Codice di condotta europeo della FEDMA (Associazione europea di Marketing diretto) per l'utilizzazione dei dati personali nel marketing diretto, venne presentata al WP29 nel 1998, ma la versione finale venne approvata solo nel 2003.[76] Una bozza di Codice di condotta per i fornitori di servizi cloud, elaborata da un gruppo di lavoro del settore creato nel 2013 e oggi sotto la presidenza congiunta di due Direzioni Generali dell'UE (DG Connect e DG Giustizia) è stata presentata al WP29 nel gennaio 2015, ma non venne approvata dal Gruppo di lavoro Articolo 29 rimanendo un "dossier *in fieri*".[77]

Sebbene non espressamente menzionato nella Direttiva, la Commissione Europea ha incentivato anche la creazione di sistemi di certificazione,[78] garantendo il finanziamento iniziale ad un gruppo di DPA e di esperti diretti dalla DPA dello Schleswig-Holstein per la creazione di un **Sistema di certificazione paneuropeo, con il marchio di certificazione *European Privacy Seal* (EuroPriSe)**, per la valutazione di prodotti e di servizi richiedenti l'utilizzo di dati personali che, se in conformità con la Direttiva (ed, eventualmente, con altri strumenti di protezione dei dati dell'UE, come la Direttiva e-Privacy, di cui parleremo nel prossimo capitolo), attribuisce un marchio di certificazione che attesta tale conformità (sebbene, vista la mancanza nella Direttiva di una base formale per un tal tipo di sistema, tali certificazioni non abbiano valore giuridico).[79]

---

[76] Testo del codice:
https://www.fedma.org/wp-content/uploads/2017/06/FEDMACodeEN.pdf
Il Parere 3/2003 sul Codice di condotta europeo della FEDMA per l'utilizzazione dei dati personali nel marketing diretto, del Gruppo di lavoro Articolo 29, che avalla il codice (WP77, adottato il 13 giugno 2003), è disponibile su:
http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp77_en.pdf

[77] Si veda:
https://ec.europa.eu/digital-single-market/en/news/data-protection-code-conduct-cloud-service-providers
(19 luglio 2013 - contesto generale e documenti di riferimento)
https://ec.europa.eu/digital-single-market/en/news/data-protection-code-conduct-cloud-service-providers
(12 ottobre 2015 - ultime informazioni disponibili)
Gruppo di lavoro Articolo 29, Parere 02/2015 del C-SIG sul Codice di condotta del Cloud Computing (WP232, adottato il 22 settembre 2015), consultabile su:
http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf
Per maggiori dettagli e considerazioni alla luce del RGPD, si veda la lettera inviata dal WP29 all'associazione dei fornitori di servizi di infrastrutture cloud (Cloud Infrastructure Services Providers) europei, del 6 febbraio 2018, consultabile qui: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=61503 .

[78] Con l'emergere e l'affermarsi di Internet all'inizio degli anni '90, la DPA francese suggerì alle altre DPA europee e alla Commissione Europea che i dispositivi di certificazione potessero costituire dei mezzi molto efficaci per gestire i servizi online stabiliti al di fuori dei confini europei. All'epoca non venne comunque intrapresa alcuna iniziativa.

[79] Si veda:
https://www.european-privacy-seal.eu/EPS-en/about-europrise

*NUOVO Norme sul "diritto nazionale applicabile"

Come emerge chiaramente dall'articolazione delle varie rubriche di cui sopra, la Direttiva garantisce agli Stati membri un notevole potere discrezionale nella determinazione delle modalità di "recepimento" delle disposizioni della Direttiva, che lascia liberi quest'ultimi di adottarne le norme alle condizioni che ritengono appropriate al loro specifico contesto. Questo ha generato una grave mancanza di armonizzazione[80] – uno dei motivi principali per cui si è scelto il Regolamento quale forma giuridica destinata a sostituire la Direttiva.[81]

Le difficoltà causate da tali discrepanze sono state, in un certo modo, superate grazie alla fondamentale disposizione contenuta nella Direttiva sulla protezione dei dati del 1995 e relativa al "diritto nazionale applicabile". La norma, di cui all'Art. 4, in effetti stabilisce tre diverse disposizioni per il settore privato:

(1) i titolari del trattamento che effettuano le loro attività nel territorio di un unico Stato membro devono rispettare la legislazione sulla protezione dei dati di tale Stato membro per ogni trattamento "effettuato nel contesto delle attività di uno stabilimento di [tale] titolare" (Art. 4(1)(a), prima parte dell'enunciato);

(2) i titolari del trattamento che effettuano le loro attività nel territorio di più di uno Stato membro [cioè: uno stesso titolare che è stabilito nel territorio di più Stati membri] devono adottare "le misure necessarie per assicurare l'osservanza, da parte di ciascuno di detti stabilimenti, degli obblighi stabiliti dal diritto nazionale applicabile" (parliamo quindi del diritto del paese in cui è stabilità l'attività in questione) (Art. 4(1)(a), seconda parte dell'enunciato);

(3) i titolari del trattamento che non sono stabiliti nel territorio della Comunità (UE) devono rispettare le legislazioni nazionali dello Stato membro sul cui territorio "utilizzano strumenti, automatizzati o non automatizzati" (Art. 4(12)(c)); tali titolari devono "designare un rappresentante stabilito" nel territorio di detto Stato membro (Art. 4(2)).[82]

Vale la pena notare che, alla luce di queste disposizioni, non soltanto i dati dei cittadini di Stati membri dell'Ue risultavano protetti da eventuali violazioni dei diritti di protezione dati commesse da soggetti extra-Ue, ma anche i **dati di tutti gli interessati** ("persone fisiche") oggetto di trattamento da parte di titolari dovevano essere protetti, ***indipendentemente dal fatto che i soggetti interessati si trovassero nell'UE o al di fuori di essa, e fossero o meno***

---

80 Si veda lo studio di Douwe Korff per la Commissione Europea, Relazione su uno studio dell'Unione Europea riguardante l'attuazione della Direttiva sulla protezione dei dati del 1995, 2002, disponibile su: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667 –

81 Si veda la Seconda Parte, sezione 2.1 e il testo del primo capoverso, "*Un Regolamento …*" alla sezione 2.2, *infra*.

82 L'applicazione di questa terza disposizione è stata complicata dall'uso di termini diversi nelle differenti versioni linguistiche (tutte facenti egualmente fede). La direttiva è stata redatta originariamente in francese, e utilizzava il termine *moyens*, in inglese "means". Il termine utilizzato nelle altre versioni linguistiche ufficiali dei paesi di lingua romanza era l'equivalente linguistico anch'esso significante "means", cioè "mezzi". Nella versione ufficiale in lingua tedesca si utilizzava il termine "Mittel", ossia di nuovo "mezzi". Tuttavia, il testo inglese parla di "*equipment*" (attrezzature), e lo stesso avviene nella versione olandese (*middelen*). Questo ha spinto il Regno Unito e i Paesi Bassi a limitare l'applicazione della norma a situazioni in cui il responsabile del trattamento, non stabilito sul territorio dell'UE/SEE, *deve possedere delle attrezzature* nell'UE/SEE (*nello specifico,* nel Regno Unito), mentre in altri paesi la sola presenza di uno smartphone nell'UE/SEE è sufficiente perché qualsiasi titolare che lo "utilizzi" per trametterе dati sia soggetto alla Direttiva.

cittadini dell'UE o ivi residenti– in linea con il principio di *universalità dei diritti umani*.[83]

Queste disposizioni, nella pratica, erano di difficile applicazione (soprattutto rispetto a titolari del trattamento stabiliti al di fuori dei territori dell'UE/SEE),[84] pur fornendo, quantomeno, alcune linee guida per affrontare normative diverse nei differenti Stati membri che potevano, in teoria, essere di applicazione ad ogni attività transnazionale di trattamento dei dati personali. La Convenzione sulla protezione dei dati del 1981 non conteneva alcuna norma volta ad evitare "conflitti di leggi".

Per quanto riguarda il settore pubblico, la determinazione del diritto nazionale applicabile è stata, nella pratica, più diretta: tutte le autorità e gli organismi pubblici, comprese le istituzioni diplomatiche sono soggette solo alla (e) legislazione (i) sulla protezione dei dati dello Stato membro in cui sono stabilite.

*NUOVO Autorità di controllo

Un'altra novità di rilievo della Direttiva del 1995, rispetto alla Convenzione del 1981,[85] è rappresentata dalla richiesta che tutti gli Stati membri nominino:

> "una o più autorità pubbliche incaricate di sorvegliare l'applicazione, sul proprio territorio, delle disposizioni di attuazione della presente direttiva, attuate dagli Stati membri".
>
> (Art. 28(1), primo capoverso)

Per operare efficacemente, tali "**autorità di controllo**" – comunemente chiamate ***Autorità per la protezione dei dati*** o ***DPA*** – (delle quali ve ne erano già diverse negli Stati membri dell'UE a ordinamento federale), dovevano disporre, in particolare, di ampi poteri ***investigativi, di intervento e di indirizzo*** (compresi quelli di ordinare il congelamento, la cancellazione o la distruzione dei dati, o quello di vietare un trattamento) (Art. 28(3), primo e secondo capoverso), ed essere "*pienamente indipendenti nell'esercizio delle funzioni loro attribuite*" (Art. 28(1), secondo punto). Il requisito dell'indipendenza è, fra l'altro, un requisito democratico e proprio di ogni Stato di diritto. Poiché la direttiva non precisava quali fossero tali requisiti di indipendenza, la Commissione ha dovuto ricorrere dinanzi alla Corte di giustizia nei confronti di vari Stati membri per fare chiarezza in merito. La relativa giurisprudenza trova rispecchiamento nelle disposizioni molto più dettagliate contenute sul punto nel RGPD.

Si prevede l'obbligo che le autorità vengano ***consultate*** dallo Stato membro al momento dell'elaborazione delle misure regolamentari o amministrative relative alla protezione dei dati (Art. 28(2)) e che dispongano del potere "***di promuovere azioni giudiziarie***" in caso di

---

83 Si veda Douwe Korff, Maintaining Trust in a Digital Connected Society, relazione per il Sindacato Internazionale delle Telecomunicazioni (ITU), maggio 2016, sezione 2.3, *Universalità dei diritti umani*, su: http://www.itu.int/en/ITU-D/Conferences/GSR/Documents/ITU_MaintainingTrust_GSR16.pdf

84 Si veda: Douwe Korff, *Der EG-Richtlinienentwurf über Datenschutz und "anwendbares Recht"*, in: Recht der Datenverarbeitung, Anno 10 (1994), Vol. N°. 5- 6, p. 209 e ss; *Il problema del "diritto applicabile"*, in: Compliance Guide 3 – Interim report (parte del of the New UK Data Protection Act 1998 Information & Compliance Programme), Privacy Laws & Business, novembre 1999.

85 La possibilità era già prevista dalle Linee guida dell'ONU, non vincolanti, adottate nel 1990 (si veda la nota 41, *supra*). Inoltre, come rilevato al punto 1.2.3, *supra*, la richiesta che gli Stati membri dispongano la creazione di autorità di controllo indipendenti, modellate su quanto stabilito dalla Direttiva sulla protezione dei dati personali del 1995, figurava già nella Convenzione del 1981 e nel Protocollo Addizionale a tale Convenzione del 2001, redatto allo scopo di allineare su questo punto il regime della Convenzione a quello della Direttiva CE del 1995 (si veda l'Art. 1 del Protocollo) – sebbene tale disposizione sia di applicazione solo per gli Stati firmatari della Convenzione che abbiano sottoscritto anche il Protocollo (come specificato alla nota 46, *supra*)

violazione delle disposizioni nazionali di attuazione della Direttiva (Art. 28(3), terzo capoverso).

Come vedremo nel prossimo punto, le autorità venivano investite anche del potere di notificazione e "controllo preliminare".

Di grande importanza è anche il fatto che, oltre alle misure formali di ricorso di cui parleremo nella prossima sottorubrica, le DPA abbiano il diritto di "**esaminare ricorsi [si intenda: trattare reclami] di qualsiasi persona interessata**, o dell'associazione che la rappresenti" in relazione alla protezione dei dati personali (Art. 28(4)).

Le DPA, le quali a livello UE lavorano con il "**Gruppo di Lavoro Articolo 29**" (WP29), e di cui si parlerà all'ultima sottorubrica della presente sezione, sono diventate i principali difensori dei diritti sulla protezione dei dati nell'UE (anche se i poteri di cui godono e l'efficacia che esprimono ai sensi delle legislazioni nazionali adottate con il recepimento della Direttiva variano di molto).

*NUOVO Notificazione e "controllo preliminare"

*NUOVO *Notificazione:*

Per ottenere una **generale trasparenza** sul trattamento dei dati personali e un pieno rispetto della legislazione sulla protezione dei dati, la Direttiva sulla protezione dei dati del 1995 stabiliva un articolato sistema di **notificazione** delle operazioni di trattamento dei dati personali (Art. 18; si veda l'Art. 19 per i dettagli dei contenuti delle notificazioni), sancendo che gli elementi di tale notificazione fossero inseriti in un **registro *consultabile da chiunque*** (Art. 21(2)). Si tratta di un sistema che si basa su quello che venne adottato in Svezia per la prima volta nel 1973, poi fatto proprio da molti Stati membri a partire da quella data.

La Direttiva, comunque, accordava agli Stati membri, come strumento alternativo alla notificazione, quello di prevedere ***semplificazioni*** o ***esenzioni*** dall'obbligo generale di notificazione e questo (soprattutto) in due tipologie "equivalenti" di casi:[86]

- qualora, in caso di un trattamento "che non rechi pregiudizio",[87] la DPA di uno Stato membro avesse varato "***norme semplificate***" che definissero i parametri di base per il trattamento (per es., la finalità del trattamento, i dati o le categorie dei dati trattati, la categoria o le categorie delle persone interessate, i destinatari o le categorie di destinatari cui sono comunicati i dati e il periodo di conservazione dei dati) (Art. 18(2), primo trattino), per cui i titolari che dichiarassero formalmente di rispettare tali norme semplificate sarebbero stati **esentati** dalla notificazione; oppure
- laddove la legislazione dello Stato membro prevedesse la nomina di un ***incaricato della protezione dei dati*** (ovvero Data Protection Officer, o DPO) indipendente, designato dal titolare del trattamento e demandato ad "assicurare in maniera indipendente l'applicazione interna [delle disposizioni nazionali di attuazione della presente direttiva] e tenere un registro dei trattamenti effettuati dal titolare del

[86] Altri trattamenti che possono essere esonerati dall'obbligo di notificazione sono **i registri pubblici** e il trattamento di dati relativi a **membri ed associati di organizzazioni no profit a carattere politico, religioso, filosofico o sindacale (salve determinate garanzie),** e **i trattamenti non-automatizzati** (Art. 18(3) – (5)).

[87] Testo completo: "Qualora si tratti di categorie di trattamento che, in considerazione dei dati oggetto di trattamento, non siano tali da recare pregiudizio ai diritti e alle libertà della persona interessata".

trattamento" contenente le stesse informazioni che altrimenti sarebbero state notificate alla DPA (Art. 18(2), secondo trattino).

La prima eccezione si basava sul sistema francese di "*normes simplifiées*"; la seconda, sul sistema tedesco che prevede la nomina di un RPD in tutti gli organismi pubblici – e in quelli privati di maggiori dimensioni-.[88] Per quanto riguarda i due sistemi, la Direttiva stabilisce che i titolari dei trattamenti (o altro organismo designato da uno Stato membro) comunichino e rendano disponibili pubblicamente le stesse informazioni che sarebbero state accessibili attraverso il registro dei trattamenti notificati (Art. 21(3)).

*NUOVO *"Controllo preliminare":*

Seguendo l'approccio francese, la Direttiva del 1995 stabiliva che i trattamenti che "**potenzialmente presentano rischi specifici per i diritti e le libertà delle persone**" ("**trattamenti rischiosi**") fossero messi in atto previo un "**controllo preliminare**"(Art. 20). Agli Stati membri era stata data facoltà di stabilire **quali tipologie di trattamenti** dovessero essere oggetto di questa disposizione (tenendo conto dello scopo del trattamento, del tipo di dati trattati, del tipo di trattamento applicato). Gli Stati membri potevano scegliere, inoltre, **come e da chi** questo controllo dovesse essere effettuato:

- con la previsione dell'obbligo di chiedere un controllo preventivo all'atto della ***presentazione di una notificazione***, specificando che il trattamento oggetto della notificazione era tale da richiedere il controllo da parte della DPA (questo era il modello francese, seguito dalla maggioranza degli altri Stati membri); oppure
- nel caso di trattamenti la cui disciplina dovesse essere fissata in norme primarie o secondarie, prevedendo che la DPA intervenisse durante il processo di preparazione dello strumento normativo, ovvero che vi provvedesse il Parlamento durante il processo di adozione di tale strumento (Art. 20(2) and (3)).

A causa delle diverse opzioni offerte dalla Direttiva, gli Stati membri hanno adottato (o, piuttosto, conservato) regimi diversi, con il risultato che trattamenti soggetti a notificazioni o controlli preliminari in alcuni Stati non lo sono stati in altri.

* Strumenti di ricorso e sanzioni specifici

La Convenzione del 1981 sanciva che gli Stati firmatari si impegnavano a "*stabilire **sanzioni e strumenti di ricorso appropriati***" per le violazioni delle disposizioni di diritto interno a protezione dei dati personali, senza peraltro chiarire cosa dovesse essere considerato "appropriato" in tal senso.

Rispetto al dettato della Convenzione del 1981, invece, la Direttiva del 1995 stabilisce che chiunque debba disporre di un **ricorso giurisdizionale** in caso di violazione (presunta) dei propri diritti (fatti salvi i ricorsi amministrativi che possono essere promossi dinnanzi all'autorità nazionale di protezione dei dati, come rilevato nella precedente sottorubrica)

[88] Denominati rispettivamente *behördliche e betriebliche Datenschutzbeauftragten*, da non confondere con le autorità di protezione dei dati statali o federali, *Landes-* e *Bundesdatenschutzbeauftragten*. Si osservi che, nonostante in molti Stati membri fosse stato introdotto il principio della designazione di un DPO attraverso le leggi nazionali di recepimento della direttiva, le relative disposizioni erano assai divergenti e prevedevano compiti e ambiti di attività diversi per i DPO nonché diverse condizioni per la loro designazione. Come vedremo nella Parte II, il RGPD prevede invece norme specifiche e armonizzate sulla designazione dei DPO e collega queste figure al principio di "responsabilizzazione".

(Art. 22). Inoltre, chiunque subisca un danno cagionato da un trattamento illecito o da qualsiasi altro atto incompatibile con le disposizioni della Direttiva ha il diritto di ottenere il **risarcimento** del pregiudizio dal titolare del trattamento (a meno che questi non provi che l'evento dannoso non gli è imputabile) (Art. 23).[89] Oltre a tali ricorsi, gli Stati membri adottano "misure appropriate" e "sanzioni", a prescindere da ogni denuncia o reclamo presentato da un singolo (Art. 24).

Va detto che in molti Stati membri, comunque, le sanzioni che possono essere imposte ai sensi della legislazione nazionale, o sono state imposte nella pratica, sono risultate molto più limitate.[90]

*NUOVO Il Gruppo di lavoro Articolo 29 e il Comitato Articolo 31

In ultimo, la Direttiva sulla protezione dei dati del 1995 stabiliva la creazione di due organismi a livello UE denominati in riferimento agli articoli che ne stabilivano la creazione:

- il cosidetto "**Gruppo di lavoro Articolo 29**", un gruppo di lavoro indipendente composto da rappresentanti delle Autorità per la protezione dei dati degli Stati membri, dal Garante europeo della protezione dei dati (GEPD) e da un rappresentante della Commissione Europea (responsabile delle funzioni di segretariato per il gruppo, senza diritto di voto), con il compito di contribuire ad un'applicazione più armonizzata della Direttiva in particolare attraverso l'adozione di raccomandazioni e pareri (d'iniziativa) nonché di emanare pareri sui progetti di codici di condotta presentati a livello Ue; la Commissione Europea aveva l'obbligo di consultare il Gruppo su ogni proposta in materia di "*diritti e libertà delle persone fisiche nel trattamento dei dati personali delle stesse*" (cioè di protezione dei dati) e su ogni bozza di decisione relativa all'adeguatezza della protezione in un paese terzo;[91]
- il cosidetto "**Comitato Aticolo 31**", composto da rappresentanti del Governo degli Stati membri, ma presieduto da un rappresentante della Commissione, cui si faceva obbligo di presentare un parere su tutte le misure da intraprendere ai sensi della Direttiva; in caso di parere negativo del Comitato, tali misure dovevano essere discusse al Consiglio e potevano essere annullate a maggioranza qualificata.[92]

Il **Gruppo di lavoro Articolo 29** (WP29) ha elaborato **numerosi pareri e documenti di lavoro** su un ampio ventaglio di problematiche in materia di applicazione della Direttiva sulla protezione dei dati del 1995 e sulla Direttiva e-Privacy del 2002 (di cui parleremo al punto 1.3.3, *infra*).[93] Questi documenti, e soprattutto i pareri formali, anche se non vincolanti, sono

---

89 Inizialmente, il Regno Unito cercò di limitare il pregiudizio ai soli danni materiali, ma si stabilì che la Direttiva dovesse garantire alle persone fisiche anche risarcimenti per danni immateriali (stress negativo).

90 La necessità di sanzioni maggiori si manifestò solo con l'emergere di Internet, largamente sotto il controllo di entità non EU/SEE che avrebbero, con minore probabilità, rispettato le disposizioni di protezione dei dati dell'UE su semplice richiesta delle DPA europee. Questa situazione ha determinato norme più severe nel RGPD: le DPA possono comminare sanzioni amministrative fino a €10.000.000 o il 2% del fatturato annuo dell'attore responsabile, oppure, in casi di particolare gravità, fino a €20.000.000 o il 4% del fatturato annuo (Art. 83 RGPD).

91 Per i dettagli, si veda l'Articolo 30.

92 Per i dettagli, si veda l'Articolo 31.

93 Tutti i documenti del Gruppo di lavoro Articolo 29 adottati fra il 1997 e il novembre 2016 possono essere consultati come materiale di archivio alla pagina:
http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm

ancora oggi testi di grande autorevolezza per le Direttive ed hanno favorito la piena e scrupolosa osservanza dell'applicazione della Direttiva ad "alto livello", mitigando, nel contempo, i problemi derivanti dalle divergenze legislative tra gli Stati membri.

NB: il successore del WP29, il Comitato europeo della protezione dei dati (EDPB), basa le proprie attività sul lavoro del WP29: nel primo giorno di esistenza, infatti, il 25 maggio 2018, ha confermato un gran numero di pareri del WP29 elaborati in previsione dell'applicazione del RGPD. Il Segretariato del Comitato è fornito dal GEPD.

1.3.3 La Direttiva sulla protezione dei dati nelle telecomunicazioni del 1997, la Direttiva e-Privacy CE del 2002, e gli emendamenti del 2009 alla Direttiva e-privacy

Quadro generale

La **Direttiva sulla protezione dei dati nelle telecomunicazioni**, proposta in contemporanea alla Direttiva sulla protezione dei dati del 1995, fu adottata il 15 dicembre 1997.[94] La sua relazione con la Direttiva sulla protezione dei dati del 1995 è chiarita all'Articolo 1(2), che afferma che le sue disposizioni sono finalizzate a "*precisare ed integrare*" la Direttiva del 1995. In particolare, le definizioni specifiche alla protezione dei dati nella Direttiva del 1995, e tutti gli altri principi e norme che figurano in questa Direttiva, sono di applicazione anche ai titolari e alle operazioni di trattamento cui si applica la Direttiva sulla protezione dei dati nelle telecomunicazioni, a meno che quest'ultima stabilisca norme più specifiche. Inoltre, per quanto riguarda scopi, elementi o servizi specifici (fatturazione dettagliata, identificazione della linea chiamante, elenchi di abbonati, ecc.), le disposizioni pertinenti costituiscono nella loro interezza interpretazioni e applicazioni dei principi generali e dei diritti fissati dalla direttiva del 1995. In altri termini, la Direttiva sulla protezione dei dati nelle telecomunicazioni elettroniche costituiva una *lex specialis* rispetto alla Direttiva sulla protezione dei dati del 1995, *lex generalis*.

Il recepimento di questa Direttiva subì ritardi dovuti in parte al fatto che, nel 1999, la Commissione decise di intraprendere una revisione generale del quadro di regolamentazione delle comunicazioni elettroniche alla luce delle nuove tecnologie e prassi aziendali in via di definizione. Uno dei risultati della revisione fu la proposta, nel 2000, di sostituzione della Direttiva sulla protezione dei dati nelle telecomunicazioni con una nuova Direttiva

---

Aggiornamenti e documenti adottati dopo il novembre 2016, all'abolizione del WP29 il 25 maggio 2018, possono essere consultati su:
http://ec.europa.eu/newsroom/article29/news-overview.cfm

[94] Titolo completo: 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 (direttiva relativa alla vita privata e alle comunicazioni elettroniche), GU L24, 30.01.1998, pp. 1 – 8, disponibile su:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31997L0066&from=EN
La Direttiva protezione dei dati personali nelle comunicazioni elettroniche attinge ampiamente all'attività del Consiglio d'Europa su una raccomandazione, riguardante la stessa problematica, che ha portato all'adozione della Raccomandazione n°R (95) 4 del Comitato dei ministri agli Stati membri relativa alla protezione dei dati a carattere personale nella gestione dei servizi di telecomunicazione, con particolare riguardo ai servizi telefonici, afottata il 7 febbraio 1995, disponibile su:
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168050108e – e al lavoro del *Gruppo di lavoro internazionale sulla protezione dei dati nel settore delle telecomunicazioni* (il "Gruppo di Berlino"), creato nel 1983, si veda:
https://www.dataprotectionauthority.be/berlin-group

riguardante la protezione dei dati nel settore delle comunicazioni elettroniche.[95] Questo portò all'adozione, nel luglio 2002, della Direttiva sulla tutela della vita privata nel settore delle comunicazioni elettroniche, la Direttiva 2002/58/CE, abitualmente definita "**Direttiva e-Privacy**".[96] Anche questo testo sottolineava il suo carattere subordinato e complementare rispetto alla Direttiva sulla protezione dei dati personali del 1995, negli stessi termini usati nei testi precedenti (si veda Art. 1(2)).

Nel 2009, la direttiva del 2002 è stata emendata da una diversa direttiva (Direttiva CE 2009/136)[97], spesso indicata come "la norma sui cookie" perché ha disciplinato i cookie – anche se in realtà ha introdotto disposizioni su altre materie e attività connesse alla protezione dei dati. Nei paragrafi seguenti si descriveranno le norme contenute nella direttiva del 2002 come emendata dalla direttiva del 2009. Per brevità parleremo della Direttiva sulla protezione dei dati del 1995 come della "Direttiva principale" (o "madre"), e della Direttiva e-Privacy (e suoi emendamenti) come della Direttiva "sussidiaria".

A oggi (dicembre 2018) la Direttiva e-Privacy è ancora in vigore, anche se la Direttiva "madre", la Direttiva sulla protezione dei dati del 1995, è stata sostituita dal Regolamento Generale sulla Protezione dei Dati (RGPD); è in fase di adozione il testo che dovrebbe sostituire la Direttiva e-Privacy e che dovrebbe prendere anch'esso la forma di un regolamento (piuttosto che di una direttiva) (si veda la sezione 1.4.2, *infra*). Tuttavia, poiché la direttiva e-privacy è ancora vigente le viene dedicato uno spazio importante in questa prima edizione del Manuale; cosicché, in attesa dell'adozione del nuovo Regolamento e-Privacy, parleremo di seguito della Direttiva e-Privacy, tuttora in vigore, utilizzando i tempi verbali al presente.

Obiettivi, finalità e campo di applicazione della Direttiva e-Privacy del 2002 come emendata nel 2009

Mentre la Direttiva sulla protezione dei dati personali del 1995 prevedeva un ampio campo di applicazione a tutti i trattamenti di dati personali da parte di organismi pubblici o privati operanti nel "Primo Pilastro" della Comunità Europea, la Direttiva e-Privacy, in quanto strumento sussidiario, ha un campo di applicazione molto più ristretto. Essa si applica al

trattamento dei dati personali **connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione** nella Comunità, *comprese le reti di comunicazione pubbliche che*

95 Proposta di direttiva del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, Bruxelles, 12.07.2000, COM(2000) 385 finale.

96 Titolo completo: 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 (direttiva relativa alla vita privata e alle comunicazioni elettroniche), GU L201, 31.07.2002, pp. 37 – 47, disponibile su:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN

97 In esteso: "Direttiva 2009/136/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 25 novembre 2009 recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori".

supportano i dispositivi di raccolta e di identificazione dei dati

(Art. 3(1), grassetti aggiunti; la frase in corsivo è stata aggiunta dalla direttiva del 2009).[98]

L'espressione "servizio di comunicazione elettronica" è definita con precisione all'articolo 2, lettera c), della Direttiva quadro[99] modificata:

«servizio di comunicazione elettronica», i servizi forniti di norma a pagamento consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, ma ad esclusione dei servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica o che esercitano un controllo editoriale su tali contenuti; **sono inoltre esclusi i servizi della società dell'informazione di cui all'articolo 1 della direttiva 98/34/CE[100] non consistenti interamente o prevalentemente nella trasmissione di segnali su reti di comunicazione elettronica**;

Il WP29, nel Parere del 2011 sui servizi di geolocalizzazione offerti su dispositivi mobili intelligenti[101], ha tratto quindi la logica conclusione, sulla base delle previsioni dell'Art. 3 e delle definizioni di cui sopra, che la direttiva e-privacy si applica ai fornitori di servizi di comunicazione elettronica quali gli operatori telecom e i fornitori di accesso a Internet, e non in relazione a fornitori di servizi della *società dell'informazione*.[102]

Come vedremo nella sezione 1.4.2, *infra*, la Commissione propone di eliminare questa restrizione nella proposta di Regolamento e-Privacy; fino ad allora, essa continua ad esplicare i propri effetti.

All'interno di questo campo di applicazione più ristretto, la direttiva e-privacy persegue gli stessi obiettivi della direttiva madre: assicurare, al contempo, un livello elevato di protezione per i dati personali (ma in questo caso specificamente nel settore considerato) e consentire la libera circolazione dei dati personali all'interno della Comunità (sempre con riguardo al settore considerato) (v. Art. 1, paragrafo 1). La direttiva ha avuto un impatto importante sul settore delle comunicazioni elettroniche, sempre in rapida crescita anche in termini di importanza, garantendo un livello più elevato di protezione dei dati in questo ambito rispetto

---

98 L'eccezione prevista nella versione originale della direttiva per le centrali telefoniche analogiche è stata soppressa con gli emendamenti del 2009.

99 Titolo completo: Direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro), GU L108, 24.04.2002, pp. 33 – 50, disponibile su: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0021&from=EN

100 Titolo completo: Direttiva 98/34/CE del Parlamento europeo e del Consiglio del 22 giugno 1998 che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche GU L 204, 21.7.1998, p. 37–48, disponibile su: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A31998L0034

101 Parere 13/2011 sui servizi di geolocalizzazione su dispositivi mobili intelligenti del Gruppo di lavoro Articolo 29 (WP185, adottato il 16 maggio 2011), sezione 4.2.1, *Applicabilità della Direttiva e-privacy modificata* (pp. 8 – 9), disponibile su: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf

102 Come ancor meglio precisato nel Documento di lavoro della Commissione (v. nota 99 *supra*), "Per ricadere nel campo di applicazione della direttiva: 1) il servizio deve essere un servizio di comunicazione elettronica; 2) il servizio deve essere offerto in una rete di comunicazioni elettroniche; 3) il servizio e la rete di cui sopra devono essere disponibili pubblicamente; e 4) la rete o il servizio devono essere forniti nella Comunità" (p. 20).
Come meglio illustrato nella sezione 1.4.2, la Commissione propone di eliminare questa limitazione nel futuro regolamento e-privacy; fino ad allora, essa continua ovviamente a esplicare i propri effetti.

ad altre regioni del mondo.

Ciò premesso, nonostante la formulazione apparentemente chiara dell'Articolo 3, la delimitazione del campo specifico di applicazione della direttiva e-privacy presenta margini di incertezza poiché alcune delle disposizioni della direttiva si applicano (anche in via interpretativa) in misura più ampia. Questo dipende in parte dal fatto che la direttiva e-privacy non contiene una disposizione specificamente riferita al diritto applicabile. Pur non volendo sminuire la validità della direttiva e-privacy, è opportuno rilevare sinteticamente alcune di queste ambiguità.

Ambiguità e incoerenze relative al campo di applicazione

Ambiguità relative al campo di applicazione materiale

In primo luogo, non è chiaro il campo di applicazione materiale della direttiva e-privacy.

Come sottolineato dalla Commissione nella proposta di regolamento e-privacy,[103]

I consumatori e le imprese si sono affidati sempre più ai nuovi servizi basati su internet intesi a consentire le comunicazioni interpersonali, quali il voice-over-IP, la messaggistica istantanea e i servizi di posta elettronica basati sulla rete anziché fruire dei servizi di comunicazione tradizionali. Questi servizi di comunicazione *over-the-top* ("**OTT**") non sono di norma soggetti all'attuale quadro di riferimento dell'Unione per le comunicazioni elettroniche, compresa la direttiva sulla vita privata elettronica.

Uno studio del 2013 commissionato dalla Commissione (Studio SMART) ha rilevato quanto segue:[104]

Le disposizioni nazionali adottate ai sensi della direttiva e-privacy e concernenti materie quali cookies, dati relativi al traffico e all'ubicazione, o le comunicazioni indesiderate, hanno spesso un campo di applicazione diverso da quello previsto all'Art. 3 della direttiva e-privacy, che è rivolta esclusivamente ai fornitori di servizi di comunicazione elettronica accessibili al pubblico (cioè ai fornitori telecom tradizionali). [Lo studio ha rilevato] che la restrizione del campo di applicazione della direttiva ai suddetti fornitori di servizi di comunicazione elettronica è fonte di ambiguità e di potenziali disparità di trattamento qualora si concluda che i fornitori di servizi della società dell'informazione che utilizzano Internet per fornire servizi di comunicazione sono, in linea di principio, sottratti all'applicazione della direttiva stessa.

Si riscontra un deficit di chiarezza anche rispetto alla legge nazionale applicabile.

Fin quando la direttiva e-privacy non sarà sostituita dal regolamento e-privacy, come proposto, (il che potrà richiedere ancora del tempo), tutte le ambiguità e le incertezze sopra descritte resteranno in essere e continueranno a pregiudicare l'efficacia della direttiva e-

[103] Proposta di regolamento e-privacy (v. nota 170, *infra*), sezione 1.1., p. 1; grassetti aggiunti.
[104] Sintesi delle risultanze dello Studio SMART, redatta dalla Commissione; grassetto aggiunto. Vedi: "e-Privacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (SMART 2013/0071) (nel prosieguo indicato come lo "Studio SMART"): https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive-assessment-transposition-effectiveness-and-compatibility-proposed-data.

privacy.

Rapporto fra la direttiva e-privacy e il RGPD

La direttiva e-privacy si poneva in un rapporto di specialità rispetto alla legge generale costituita dalla direttiva del 1995, e dunque continua a configurarsi come *lex specialis* nei riguardi dello strumento che rappresenta il successore di tale direttiva, ossia il RGPD. Nelle materie specificamente disciplinate dalla direttiva e-privacy, quest'ultima si applica in luogo del RGPD.

Pertanto, le basi giuridiche contemplate nel RGPD non trovano applicazione qualora la direttiva e-privacy contenga norme più specifiche per il trattamento di dati personali. Per esempio, l'art. 6 della direttiva e-privacy reca un elenco specifico di basi giuridiche che legittimano il trattamento di dati relativi al traffico, compresi i dati relativi al traffico che hanno natura di dati personali, e pertanto non trova applicazione l'Art. 6 del RGPD in questi casi. Tuttavia, in tutti gli altri casi relativi al trattamento di dati personali trova applicazione il RGPD.

Quanto sopra vale anche rispetto al campo di applicazione soggettivo della direttiva e-privacy, cioè con riguardo **ai soggetti che ricadono o meno "nel campo specifico di applicazione della direttiva e-privacy"**. Alla luce del parere espresso dal WP29, secondo cui la direttiva e-privacy si applica sostanzialmente ai soli fornitori di servizi di comunicazione elettronica, e fatta eccezione per le norme speciali contenute all'art. 5, paragrafo 3, e all'art. 13 di tale direttiva, che hanno un più ampio campo di applicazione, il trattamento di qualsiasi dato, compresi quelli disciplinati in modo più specifico dalla direttiva e-privacy (come i dati relativi al traffico), svolto da soggetti diversi dai fornitori di servizi di comunicazione elettronica è disciplinato dal RGPD anziché dalle direttiva e-privacy, nonostante quest'ultima rechi disposizioni speciali con riguardo ai dati in questione.

In altri termini:

- i fornitori di servizi di comunicazione elettronica devono rispettare le norme della direttiva e-privacy con riguardo alle materie che sono disciplinate in modo più specifico in quest'ultima direttiva, e le norme del RGPD con riguardo a ogni altra materia; e
- i soggetti che non sono fornitori di servizi di comunicazione elettronica devono rispettare le norme contenute all'Art. 5, paragrafo 3, della direttiva e-privacy con riguardo all'accesso alle informazioni contenute su dispositivi, e le norme contenute all'Art. 13 della suddetta direttiva con riguardo alle comunicazioni indesiderate, mentre devono rispettare le disposizioni del RGPD con riguardo a ogni altra materia (ossia, non sono soggetti a nessun'altra disposizione della direttiva e-privacy se non nei due ambiti sopra ricordati).

In altri sotto-paragrafi di questa sezione saranno esaminate le questioni specifiche che emergono in rapporto alle problematiche sopra evidenziate.

Caratteristiche principali della Direttiva e-Privacy[105]

Definizioni

Poichè la Direttiva e-Privacy è stata espressamente concepita quale *lex specialis* rispetto alla l*ex generalis* della Direttiva sulla protezione dei dati del 1995, le **definizioni relative alla protezione dei dati** della Direttiva del 1995 erano applicabili anche alla Direttiva e-Privacy, come previsto espressamente all'Art. 2, primo periodo, di quest'ultima. Tuttavia, ora che la direttiva "madre" sulla protezione dei dati è stata sostituita dal RGPD, tutti i rinvii alle definizioni contenute in tale direttiva devono intendersi come rinvii alle corrispondenti definizioni del Regolamento (che in taluni casi risultano di fatto rafforzatee aggiornate). Questa osservazione risulta di particolare rilevanza con riguardo alla voce "Consenso", v. *infra*.[106]

A parte questo, le **definizioni di termini più tecnici e relativi alle comunicazioni elettroniche** della Direttiva quadro per le Reti ed i Servizi di Comunicazione elettronica[107], che fu il frutto della revisione di cui parlavamo prima, – definizioni quali ***servizio di comunicazione elettronica***;[108] ***servizi di comunicazione elettronica accessibili al pubblico; rete pubblica di comunicazione***, ecc. – si applicano anche ai termini tecnici fondamentali della Direttiva e-Privacy. Fra questi termini figura quello di "**abbonato**" (a un servizio di comunicazione elettronica).

Inoltre, l'Art.2 della Direttiva e-Privacy aggiunge **ulteriori definizioni**, quali quelle di "utente", "dato relativo al traffico", "dato relativo all'ubicazione", "servizio a valore aggiunto", e "violazione dei dati personali" (si veda il testo degli articoli per maggiori dettagli).

Consenso

La modifica più importante concernente i concetti-chiave del RGPD rispetto alla direttiva del 1995 riguarda la definizione di "**consenso**" in quanto base giuridica per il trattamento di dati personali.

Nello specifico, l'art. 2, lettera f), della direttiva e-privacy prevede che il "consenso" dell'utente o dell'abbonato di cui a tale direttiva corrisponde al consenso dell'interessato di cui alla direttiva sulla protezione dei dati. Poiché tutti i riferimenti alla direttiva sulla protezione dei dati devono intendersi come fatti al RGPD, il consenso di cui alla direttiva e-privacy è necessariamente da intendersi come identico al consenso di cui al RGPD, ossia come "qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di

---

105 Rileviamo, una volta per tutte, che molte delle disposizioni della Direttiva e-Privacy figuravano già nella Direttiva del 1997 sulla protezione dei dati nelle telecomunicazioni e sono state integrate, tali e quali, nella Direttiva e-Privacy. La presenza dell'indicazione "*NUOVO" accanto a una voce o disposizione significa che si tratta di un elemento non (precedentemente) disciplinato dalla direttiva sulla protezione dei dati del 1995.

106 Il RGPD chiarisce ulterioremente, in qualche misura, la nozione di "dato personale" specificando che una persona fisica è "identificabile" anche attraverso un "identificativo online" (art. 4.1 del RGPD, Art. 2, lettera (a) della Direttiva del 1995). Si tenga conto anche di questo aspetto nell'applicazione della direttiva e-privacy.

107 V. nota 99, *supra*.

108 Si veda *supra* la sezione intitolata "Obiettivi, finalità e ambito di applicazione della direttiva e-privacy".

trattamento." (Art. 4, paragrafo 11).

Il RGPD chiarisce le condizioni di validità del consenso in modo più dettagliato e specifica, fra l'altro, cosa debba intendersi per consenso "libero" e cosa rappresenta una "azione positiva inequivocabile".[109] Inoltre, il Comitato europeo per la protezione dei dati ha pubblicato specifiche linee-guida in tema di consenso.[110]

Questi elementi di chiarificazione contenuti nel RGPD risultano particolarmente pertinenti in rapporto a numerose disposizioni-chiave della direttiva e-privacy che prevedono il consenso dell'utente o dell'abbonato. Si tratta delle seguenti:

- L'art. 5.3, ai fini della memorizzazione o della raccolta di informazioni dal terminale dell'utente o dell'abbonato;
- Gli artt. 6 e 9, ai fini del riutilizzo di dati relativi al traffico e all'ubicazione per la prestazione di servizi a valore aggiunto o per la commercializzazione di servizi di comunicazione elettronica;
- L'art. 12, ai fini della creazione di elenchi di abbonati; e
- L'art. 13, ai fini delle comunicazioni indesiderate.

Nelle materie di cui sopra, la validità del consenso presuppone oggi che si tratti del "consenso di cui al RGPD" ed è necessario che gli Stati membri verifichino la legislazione nazionale di recepimento della direttiva e-privacy e le prassi nazionali di attuazione di tale legislazione al fine di garantire la loro conformità al RGPD.

Le materie di cui sopra sono analizzate in maggiore dettaglio nei paragrafi in appresso.

Sicurezza

L'Articolo 4(1) ribadisce la norma sulla sicurezza dei dati, già presente nella Direttiva del 1995, e sancisce che i fornitori di servizi di comunicazione elettronica dovono prendere "***appropriate misure tecniche e organizzative per salvaguardare la sicurezza dei propri servizi***", aggiungendo che, "*se necessario*", tale tutela va assicurata "*congiuntamente con il fornitore della rete pubblica di comunicazione*". Inoltre, come figurava nella Direttiva principale, il livello di sicurezza deve essere "***adeguato al rischio esistente***", tenuto conto delle conoscenze in materia e dei costi di realizzazione. L'Art. 4, paragrafo 1-bis, introdotto dalla Direttiva del 2009, aggiunge quanto segue:

Fatta salva la direttiva 95/46/CE, le misure dicui al paragrafo 1 quanto meno:

— garantiscono che i dati personali siano accessibili soltanto al personale autorizzato per fini legalmente autorizzati,
— tutelano i dati personali archiviati o trasmessi dalla distruzione accidentale o illecita, da perdita o alterazione accidentale e da archiviazione, trattamento, accesso o divulgazione non

[109] Si vedano gli artt. 7 e 8 RGPD e i relativi considerando (32-33 e 42-43).

[110] Linee-guida del CEPD sul consenso nel Regolamento 2016/679 (WP259rev.01). Le Linee-guida sono state adottate dal Gruppo "Articolo 29" il 28 novembre 2017 ed emendate il 10 aprile 2018. Sono state successivamente approvate dal successore del Gruppo, ossia dal Comitato europeo per la protezione dei dati. Esse integrano un precedente parere del Gruppo "Articolo 29" sulla definizione di consenso (WP187, parere 15/2011).

autorizzati o illeciti, e
— garantiscono l'attuazione di una politica di sicurezza in ordine al trattamento dei dati personali.

Sia la direttiva e-privacy (Art. 4) sia il RGPD (Artt. 32-34) prevedono un obbligo di garantire la sicurezza oltre all'obbligo di notificare le violazioni dei dati personali[111] all'autorità nazionale competente e all'autorità di controllo [cioè all'autorità di protezione dati], rispettivamente.[112] Tali obblighi esisteranno in parallelo ai sensi dei due diversi strumenti citati e in rapporto ai rispettivi ambiti applicativi. Ai sensi dell'art. 95 del RGPD, quest'ultimo non impone obblighi supplementari alle persone fisiche o giuridiche per quanto riguarda le materie per le quali sono soggette a obblighi specifici fissati nella direttiva e-privacy. Tuttavia, in quanto *lex specialis* rispetto al RGPD, la direttiva e-privacy non dovrebbe [neppure] comportare un livello di tutela inferiore rispetto a quella garantita dal RGPD.

L'art. 4, paragrafo 1-bis, prevede inoltre che

Le autorità nazionali competenti sono legittimate a verificare le misure adottate dai fornitori di servizi di comunicazione elettronica accessibili al pubblico e a emanare raccomandazioni sulle migliori prassi in materia di sicurezza che tali misure dovrebbero conseguire.

Si osservi che le "autorità nazionali competenti" non sono necessariamente le autorità nazionali di protezione dei dati. Si veda, sul punto, la sezione intitolata "Vigilanza e attuazione", *infra*.

*NUOVO Notifica del rischio

In base all'Art. 4, paragrafo 2, della direttiva e-privacy,

Nel caso in cui esista **un particolare rischio di violazione della sicurezza della rete**, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha l'obbligo di informarne gli abbonati indicando, qualora il rischio sia al di fuori del campo di applicazione delle misure che devono essere prese dal fornitore di servizio, tutti i possibili rimedi, compresi i relativi **costi** presumibili.

L'obbligo di "notificare il rischio", già previsto nel testo del 2002, va distinto dagli obblighi più articolati connessi alla "notifica delle violazioni dei dati" di cui si parlerà nel paragrafo successivo e che sono stati introdotti solo con gli emendamenti del 2009; peraltro, questi obblighi ulteriori si applicano solo dopo che si è verificata una violazione, mentre l'Art. 4, paragrafo 2, impone di notificare il rischio di una *eventuale* violazione.

*NUOVO Notifica delle violazioni dei dati

La direttiva e-privacy come modificata nel 2009 prevede che, oltre all'obbligo di notifica dei rischi sopra ricordato, i fornitori di servizi di comunicazione elettronica ***notifichino all' "autorità nazionale competente"*** ogni violazione dei dati personali (ossia, ogni *effettiva* violazione) *"senza indebiti ritardi"* (Art. 4, paragrafo 3, secondo periodo). Tuttavia, non è

[111] Si veda sul punto il paragrafo specificamente dedicato alla notifica delle violazioni dei dati personali, *infra*.
[112] Quanto alle diverse autorità coinvolte nell'attuazione della direttiva e-privacy, si vedano il brano citato più avanti in questo paragrafo e i relativi commenti, nonché le osservazioni svolte nell'ultima parte della presente sezione.

necessario effettuare tale notifica nei confronti dell'abbonato o della persona interessata

se il fornitore ha dimostrato in modo convincente all'autorità competente di aver utilizzato le opportune misure tecnologiche di protezione e che tali misure erano state applicate ai dati interessati dalla violazione della sicurezza. Tali misure tecnologiche di protezione rendono i dati incomprensibili a chiunque non sia autorizzato ad accedervi.

In altri termini, non occorre informare di una violazione dei dati gli abbonati e altre persone interessate (in particolare, come è ovvio, gli interessati dal trattamento, ma anche gli abbonati che siano persone giuridiche) se il fornitore è in grado di dimostrare alla "autorità competente" che i dati oggetto della violazione (in particolare, dati comunicati o resi accessibili impropriatemente a terze parti) erano stati resi totalmente "incomprensibili" a chiunque abbia potuto accedervi a seguito della violazione, attraverso opportune misure tecnologiche di protezione (come meglio chiarisce l'Art. 4 del Regolamento della Commissione 611/2013).[113]

Viceversa, una "Autorità competente" può "imporre" a un fornitore di notificare una violazione dei dati agli abbonati e ad altri soggetti interessati qualora tale fornitore non vi abbia provveduto – per esempio, perché l'autorità non concorda con la valutazione compiuta dal fornitore stesso secondo cui la la violazione non "rischia di pregiudicare" i dati personali o la riservatezza di tali abbonati o soggetti, oppure perché l'autorità non ritiene che alcuni dei dati oggetto della violazione siano realmente "incomprensibili" per i destinatari non autorizzati (ad esempio, perché anche la chiave di decifrazione è stata violata, oppure perché il metodo di cifratura utilizzato non era sufficientemente robusto)[114] (Art. 4, paragrafo 3, quarto capoverso).

Il quinto e ultimo capoverso dell'Art. 4, paragrafo 3, prevede quanto segue:

La comunicazione all'abbonato o ad altra persona contiene almeno una descrizione della natura della violazione di dati personali e i punti di contatto presso cui si possono ottenere maggiori informazioni ed elenca le misure raccomandate per attenuare i possibili effetti pregiudizievoli della violazione di dati personali. La comunicazione all'autorità nazionale competente descrive, inoltre, le conseguenze della violazione di dati personali e le misure proposte o adottate dal fornitore per porvi rimedio.

La direttiva e-privacy come emendata dalla direttiva del 2009 prevede, inoltre, alcuni

[113] REGOLAMENTO (UE) N. 611/2013 DELLA COMMISSIONE del 24 giugno 2013 sulle misure applicabili alla notifica delle violazioni di dati personali a norma della direttiva 2002/58/CE del Parlamento europeo e del Consiglio relativa alla vita privata e alle comunicazioni elettroniche. GU L173 del 26.06.2013, p. 2-8.
Il Regolamento è stato adottato sulla base dell'Art. 4, paragrafo 5, della Direttiva e-privacy, che autorizzava la Commissione ad adottare "*misure tecniche di attuazione riguardanti le circostanze, il formato e le procedure applicabili alle prescrizioni in materia di informazioni e comunicazioni di cui al presente articolo*." (Art. 4 paragrafo 5) previa consultazione dell'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), del WP29 e del GEPD, e con il coinvolgimento di tutte le (altre) parti interessate.

[114] Per esempio, alcuni algoritmi di cifratura come MD5 o SHA1 sono ritenuti ormai obsoleti cosicché dati crittati attraverso tali algoritmi non potrebbero più essere considerati realmente "incomprensibili" (ossia: indecifrabili). Si veda: https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet. Si pensi anche a una violazione dei dati oggetto di comunicazione elettronica in cui il contenuto della comunicazione era adeguatamente cifrato attraverso algoritmi "forti" come SHA-256, ma i metadati non lo erano. Si osservi che, come evidenziato nel testo reperibile al suddetto link, "la classificazione degli algoritmi crittografici come "forti" o meno tende a cambiare nel tempo".

importanti requisiti formali a supporto delle nuove disposizioni introdotte. In particolare:

[Le autorità nazionali competenti] possono altresì **verificare** se i fornitori hanno adempiuto ai loro obblighi di comunicazione a norma del presente paragrafo e irrogano **sanzioni** appropriate in caso di omissione. (Art. 4, paragrafo 4, primo capoverso, secondo periodo)

L'efficacia di tali verifiche (ispezioni) si appoggia a un ulteriore obbligo fissato nel secondo capoverso dell'Art. 4, paragrafo 4:

I fornitori tengono un **inventario delle violazioni dei dati personali**, ivi incluse le circostanze in cui si sono verificate, le loro conseguenze e i provvedimenti adottati per porvi rimedio, in misura sufficiente per consentire alle autorità nazionali competenti di verificare il rispetto delle disposizioni di cui al paragrafo 3. Nell'inventario figurano unicamente le informazioni necessarie a tal fine.

La direttiva e-privacy come modificata prevede, inoltre, che le "autorità nazionali competenti" emanino "orientamenti" e "istruzioni" quanto alle "circostanze in cui il fornitore ha l'obbligo di comunicare le violazioni di dati personali, al formato applicabile a tale comunicazione, nonché alle relative modalità di effettuazione." (Art. 4, paragrafo 4, primo capoverso, primo periodo).

Gli obblighi di notifica delle violazioni dei dati personali fissati dalla direttiva e-privacy, il cui ambito è limitato a quello pertinente alla direttiva stessa, prefigurano gli obblighi più generali di notifica di tali violazioni che sono oggi previsti dal Regolamento generale sulla protezione dei dati e che hanno valenza erga omnes, cioè con riguardo a ogni operazione di trattamento (v. Parte II, paragrafo 2.1). Possono ritenersi "ridondanti".[115]

Requisiti specifici del trattamento per scopi specifici:

Invece di limitarsi a riprendere i principi generali sulla protezione dei dati e la lista delle basi giuridiche di applicazione al trattamento dei dati elencate nella Direttiva principale del 1995, la Direttiva e-Privacy fissa una norma generale di riservatezza delle comunicazioni e una serie di disposizioni specifiche e condizioni per determinati dati o trattamenti. Attraverso tali disposizioni la direttiva e-privacy mira ad applicare principi e diritti fissati nella direttiva "madre" del 1995 alle specifiche materie considerate, con l'obiettivo di armonizzare l'applicazione di tali principi e diritti negli Stati membri – come meglio vedremo nei paragrafi seguenti.

In prima battuta, è però importante ricordare che le basi giuridiche del trattamento per le varie finalità di cui agli Articoli 5 e 6 del RGPD non trovano applicazione nella misura in cui la direttiva e-privacy prevede una base giuridica specifica per il trattamento avente specifiche finalità ai sensi di tale direttiva.[116]

Pertanto, ove la direttiva e-privacy prevede il requisito del consenso (per esempio ai fini dell'accesso a informazioni contenute su dispositivi dell'utente (Art. 5.3) oppure per l'invio di messaggi indesiderati di commercializzazione (Art. 13)) ovvero elenca una serie di specifiche

[115] Commissione europea: REFIT analysis of coherence of the e-Privacy Directive with the GDPR. (Grafico – commenti ad artt. 4.3; 4.4.; 4.5 – Notifica delle violazioni dei dati personali).
[116] Si veda il paragrafo dedicato al "Rapporto fra direttiva e-privacy e RGPD", *supra*.

basi giuridiche e specifiche finalità di trattamento (per esempio in rapporto al trattamento di dati relativi al traffico (Art. 6)) – chiunque sia soggetto a tali disposizioni (chiunque, effettivamente, per quanto riguarda gli Artt. 5(3) e 13, e invece solo i fornitori di servizi di comunicazione elettronica per quanto riguarda l'Art. 6) non può fare riferimento ad altri fondamenti di liceità del trattamento fissati nel RGPD. In particolare, non è possibile richiamarsi al principio di "non incompatibilità della finalità" di cui all'Art. 5, paragrafo 1, lettera b) del RGPD.

*NUOVO ***Riservatezza delle comunicazioni***

L'art. 5, paragrafo 1, della Direttiva e-Privacy mette in risalto la fondamentale importanza della riservatezza delle comunicazioni – incardinata in molte Costituzioni, almeno per quanto riguarda il servizio postale o telefonico tradizionale (un concetto che spesso è stato esteso di proposito o interpretato estensivamente fino a coprire ogni forma di comunicazione)[117] – sancendo che gli Stati membri devono:

> assicurare, mediante disposizioni di legge nazionali, la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico. In particolare essi vietano l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi, eccetto quando sia autorizzato legalmente …

Come evidenziato dall'uso di termini quali "ascolto, captazione…" ecc., "a opera di persone diverse dagil utenti", questa disposizione non si applica solo ai fornitori di servizi di comunicazione elettronica. In effetti, e salve le eccezioni indicate nel prosieguo, gli Stati membri devono vietare, con legge nazionale, tali ingerenze nel diritto alla riservatezza delle comunicazioni **da chiunque commesse**, siano essi soggetti pubblici o privati.

L'Art. 5(1) contempla l'eccezione della "memorizzazione tecnica necessaria alla trasmissione della comunicazione, fatto salvo il principio della riservatezza". Un'ulteriore eccezione figura al paragrafo (2) in relazione alla "registrazione di comunicazioni e di dati sul traffico allo scopo di fornire la prova di una transazione o di una comunicazione commerciale"). La cosidetta Direttiva sulla conservazione dei dati, di cui tratteremo brevemente nella sezione 1.3.4, *infra*, prevedeva un'ulteriore, ampia eccezione obbligatoria al divieto di intercettazione e raccolta dei dati di comunicazione, ma la norma è stata dichiarata nulla dalla Corte di Giustizia, come vedremo.

Utilizzo dei "cookie" e di altre tecnologie intrusive

All'Articolo 5(3) della direttiva e-privacy, come modificata, viene enunciato in termini piuttosto tecnici che gli Stati membri assicurano che:

> **l'archiviazione di informazioni oppure l'accesso a informazioni già archiviate**

[117] Cfr. l'interpretazione estensiva del concetto di "corrispondenza" di cui all'Art.8 della sentenza della Corte Europea dei Diritti dell'uomo -CEDU- nella famosa causa *Klass contro repubblica Federale di Germania* (sentenza del 6 settembre 1978), paragrafo 41, in cui la Corte afferma che "*le conversazioni telefoniche … rientrano nelle nozioni di 'vita privata' e 'corrispondenza' [come definite in quell'articolo]*".

> **nell'apparecchiatura terminale di un abbonato o di un utente** sia consentito unicamente a condizione che l'abbonato o l'utente in questione abbia espresso preliminarmente il proprio **consenso**, dopo essere stato **informato in modo chiaro e completo**, a norma della direttiva 95/46/CE, tra l'altro sugli scopi del trattamento.

Al periodo successivo la Direttiva chiarisce quanto segue:

> Ciò non impedisce l'eventuale memorizzazione tecnica o l'accesso al solo fine di effettuare o facilitare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria a fornire un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente (corsivi e grassetti aggiunti).

Si osservi come le espressioni "al solo fine" e "nella misura strettamente necessaria" sottolineino l'interpretazione restrittiva che deve essere adottata nell'implementare l'eccezione in questione.

La frase "l'archiviazione di informazioni oppure l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un abbonato o di un utente" si riferisce, in un linguaggio tecnico, a quelle operazioni che permettono al visitatore di un sito web di essere riconosciuto dal sito stesso e tracciato nel suo utilizzo del sito, o anche di più siti. Lo strumento più importante a tale scopo è rappresentato dai cosiddetti "cookie", ed è per tale motivo che la direttiva del 2009 con cui sono state introdotte regole più cogenti in materia (v. *infra*) è stata (e tuttora è) spesso indicata come la "norma sui cookie" dell'Ue (si veda, per esempio, come si esprime sul punto sito di un soggetto privato[118]).

In realtà, i cookie possono assumere tipologie molto diverse in base a strumenti tecnici standardizzati a livello internazionale, detti "RFC" che sono stati adottati dalla Internet Engineering Task Force (IETF). Nel linguaggio corrente, possiamo affermare che si va dai "cookie di tracciamento di terze parti", particolarmente intrusivi, a cookie non intrusivi che migliorano il funzionamento di un sito web senza tracciare il visitatore;[119] vi sono poi altre tecnologie intrusive come i "flash cookie", le tecniche di memorizzazione HTML5, e i cosiddetti "evercookie"[120]. Tutti ricadono comunque nella definizione di "informazioni

---

[118] https://www.cookielaw.org/the-cookie-law/

[119]

Si vedano le varie Raccomandazioni IETF sui cookie (a partire dalla RFC 2109 del 1997) che contengono una nozione imprecisa di privacy ma prevedono l'inserimento nei cookie in via obbligatoria di alcune utili informazioni.
https://tools.ietf.org/html/rfc2109 (la RFC 2109 originale);
https://tools.ietf.org/html/rfc2965 (RFC 2965, che ha sostituito la RFC 2109 mantenendo invariato l'elenco dei dati); e
https://tools.ietf.org/html/rfc6265 (RFC 6265 del 2011, sempre mantenendo l'elenco originario, ma con l'introduzione dell'accesso al cookie da parte di soggetti terzi; questa è la raccomandazione attualmente in vigore).
Si veda anche la seguente pagina di Wikipedia:
https://en.wikipedia.org/wiki/HTTP_cookie
Vi si trova un'ampia disamina delle varie tipologie di cookie: cookie di sessione, cookie persistenti, cookie di sicurezza, cookie esclusivamente pertinenti al protocollo http, cookie "same site", cookie di terze parti, supercookie e zombie cookie, nonché dettagliate informazioni tecniche.

[120] Si veda:
https://webcookies.org/doc/eu-web-cookies-directive.

archiviate nelll'apparecchiatura terminale" e quindi, anche se con qualche difficoltà, sono tutti trattati alla stessa stregua in base alla direttiva e-privacy.[121]

Lo scopo e il significato della disposizione di cui all'Articolo 5, paragrafo 3, sono delucidati in un linguaggio più semplice nei Considerando (24) e (25) della Direttiva e-Privacy, che chiariscono che la norma ha un'applicazione ben più ampia dei "cookie". Vale la pena citarli per intero:

> (24) Le apparecchiature terminali degli utenti di reti di comunicazione elettronica e qualsiasi informazione archiviata in tali apparecchiature fanno parte della sfera privata dell'utente, che deve essere tutelata ai sensi della convenzione europea per la protezione dei diritti dell'uomo e delle libertà fondamentali. I cosiddetti **software spia, bachi invisibili ("web bugs"), identificatori occulti ed altri dispositivi analoghi possono introdursi nel terminale dell'utente a sua insaputa al fine di avere accesso ad informazioni, archiviare informazioni occulte o seguire le attività dell'utente e possono costituire una grave intrusione nella vita privata di tale utente. L'uso di tali dispositivi dovrebbe essere consentito unicamente per scopi legittimi e l'utente interessato dovrebbe esserne a conoscenza**. (grassetto aggiunto)
>
> (25) Tuttavia, tali dispositivi, **per esempio i cosiddetti marcatori ("cookies")**, possono rappresentare uno strumento legittimo e utile, per esempio per l'analisi dell'efficacia della progettazione di siti web e della pubblicità, nonché per verificare l'identità di utenti che effettuano transazioni "on-line". Allorché tali dispositivi, ad esempio i marcatori ("cookies"), sono destinati a scopi legittimi, come facilitare la fornitura di servizi della società dell'informazione, il loro uso dovrebbe essere consentito purché siano fornite agli utenti informazioni chiare e precise, a norma della direttiva 95/46/CE, sugli scopi dei marcatori o di dispositivi analoghi per assicurare che gli utenti siano a conoscenza delle informazioni registrate sull'apparecchiatura terminale che stanno utilizzando. Gli utenti dovrebbero avere la possibilità di rifiutare che un marcatore o un dispositivo analogo sia installato nella loro apparecchiatura terminale. Ciò riveste particolare importanza qualora utenti diversi dall'utente originario abbiano accesso alle apparecchiature terminali e quindi a dati contenenti informazioni sensibili in relazione alla vita privata che sono contenuti in tali apparecchiature. L'offerta di informazioni e del diritto di opporsi può essere fornita una sola volta per l'uso dei vari dispositivi da installare sull'attrezzatura terminale dell'utente durante la stessa connessione e applicarsi anche a tutti gli usi successivi, che possono essere fatti, di tali dispositivi durante successive connessioni. Le modalità di comunicazione delle informazioni, [dell'offerta del diritto al rifiuto][122] o della richiesta del consenso dovrebbero essere il più possibile chiare e comprensibili. L'accesso al contenuto di un sito Internet specifico può tuttavia continuare ad essere subordinato all'accettazione in conoscenza di causa di un marcatore o di un dispositivo analogo, se utilizzato per scopi legittimi (grassetto aggiunto).

La modifica principale introdotta dalla direttiva del 2009 ha riguardato il regime relativo all'utilizzo di queste tecnologie: da un sistema basato sull'informazione preventiva dell'utente o dell'abbonato e sulla possibilità per questi di esercitare un "diritto di opposizione"

[121] Questo stato di cose potrebbe modificarsi con il nuovo regolamento e-privacy, che potrebbe prevedere un approccio differenziato in rapporto alla maggiore o minore intrusività delle singole tecnologie.
[122] Si vedano in proposito le due note seguenti.

all'installazione di cookie (ecc.)[123], si è passati al sistema attualmente vigente in base all'Art. 5, paragrafo 3, per cui l'installazione dei cookie è consentita solo se l'abbonato o l'utente sono stati informati preventivamente e hanno dato il proprio consenso esplicito e positivo conformemente ai requisiti di validità del consenso di cui alla direttiva "madre" del 1995[124]. In base a quest'ultima, per consenso si intende

"qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento" (Art. 2, lettera h).

Tuttavia, tenuto conto che la direttiva del 1995 è stata ora sostituita dal RGPD, si pone la questione interpretativa della natura di tale "consenso": se si tratti, cioè, del consenso avente le caratteristiche più impegnative previste dal Regolamento. Se così fosse, il consenso per l'installazione di cookie e altri dispositivi dovrebbe oggi basarsi su quanto segue:

"qualsiasi manifestazione di volontà libera, specifica, informata e **inequivocabile** [dell'abbonato o dell'utente], con la quale lo stesso manifesta il proprio assenso, **mediante dichiarazione o azione positiva inequivocabile**, che [siano installati cookie o siano utilizzati altri dispositivi]"[125]

Cò significa che l'utilizzo di caselle pre-spuntate ai fini del consenso all'uso di cookie ecc. non sarà più conforme ai requisiti fissati in merito dalla direttiva e-privacy.

Tuttavia, resta il fatto che la Direttiva e-Privacy tratta "cookie" e strumenti di tracciatura allo stesso modo, senza distinzione, ed esempio, fra "cookie di sessione" e "cookie persistenti".

In pratica, questa norma ha favorito in Internet una cultura del "prendere o lasciare" per la quale gli utenti del web sono oggi obbligati a cliccare "*Acconsento*" (all'inserimento di "cookie" di solito non meglio specificati) per avere accesso ad un sito (compresi, spesso, anche quelli di organismi pubblici).

Nello Studio SMART si è osservato che[126]

Le regole in materia di cookie e simili dispositivi non hanno probabilmente centrato appieno il loro obiettivo, visto che gli utenti ricevono troppi messaggi di notifica ai quali non prestano la dovuta considerazione.

Resta da vedere se la situazione cambierà con il nuovo regolamento e-privacy, anche se naturalmente queste tematiche sono direttamente connesse all'applicazione di tutti i principi

[123] Nella versione originale del 2002, il primo periodo dell'Art. 5(3) recava quanto segue: "Gli Stati membri assicurano che l'uso di reti di comunicazione elettronica per archiviare informazioni o per avere accesso a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente interessato sia stato **informato** in modo chiaro e completo, tra l'altro, sugli scopi del trattamento in conformitàdella direttiva 95/46/CE e che gli sia offerta **la possibilità di rifiutare** tale trattamento da parte del responsabile del trattamento. Ciò non impedisce l'eventuale memorizzazione tecnica o l'accesso al solo fine di effettuare o facilitare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria a fornire un servizio della societàdell'informazione esplicitamente richiesto dall'abbonato o dall'utente."

[124] In effetti queste modifiche non sono rispecchiate dai considerando qui citati, che non sono stati emendati rispetto al testo originario del 2002 e continuano a utilizzare l'espressione "possibilità di rifiutare" pur essendo quest'ultima opzione scomparsa con le modifiche apportate dalla direttiva del 2009. Si tratta, dunque, di espressioni destinate a restare lettera morta.

[125] V. Art. 4(11) del RGPD.

[126] V. nota 104 *supra*.

e i diritti fondamentali in materia di protezione dei dati – fra cui i principi di limitazione della finalità, minimizzazione dei dati, limitazione della conservazione, ecc. .- Si pensi a questioni quali la definizione dei periodi di conservazione adeguati per le varie tipologie di cookie (in rapporto alla rispettiva finalità)[127], le modalità di ottenimento di un consenso valido ("consenso di cui al RGPD") per l'utilizzo dei vari tipi di cookie, i meccanismi atti a garantire l'esercizio dei diritti da parte degli interessati, e così via. Più in generale, si tratterà di definire in che modo tutto ciò possa e debba trovare attuazione sulla base dei principi di protezione dei dati per impostazione predefinita e fin dalla fase di progettazione – principi oggi espressamente sanciti dal RGPD.

*NUOVO *Limitazioni ai dati sul traffico e ai dati relativi all'ubicazione*

L'Art. 6 della Direttiva e-Privacy impone severe limitazioni e restrizioni al trattamento dei dati sul traffico e dei dati relativi all'ubicazione da parte dei fornitori di servizi di comunicazione elettronica. In linea di principio, **i dati sul traffico** (cioè i dati elaborati allo scopo di, e necessari a, una comunicazione o l'invio di una fattura) possono essere elaborati e immagazzinati solo da un fornitore di servizi di comunicazione elettronica per la ***trasmissione*** di una comunicazione elettronica, la ***fatturazione*** all'abbonato della comunicazione o l'***interconnessione di pagamenti*** (come, ad esempio, i pagamenti fra fornitori per l'utilizzo delle reti di altri fornitori) (Art. 6(1) e (2)). Questi trattamenti non necessitano del consenso da parte dell'abbonato o del'utente del servizio in quanto necessari ai fini della prestazione del servizio. Quando non più necessari a tali fini, questi dati devono essere "cancellati o resi anonimi" (Art. 6(1)).[128]

I dati sul traffico possono essere utilizzati solo per il ***marketing di servizi di comunicazioni elettroniche*** o per la fornitura di servizi a ***valore aggiunto,*** ma solo con il **consenso** dell'abbonato o dell'utente. Ancora una volta, ciò significa che, alla luce della piena applicabilità del RGPD, deve trattarsi di un consenso conforme ai requisiti di validità fissati nel RGPD, ossia deve trattarsi di una

> manifestazione di volontà libera, specifica, informata e inequivocabile [dell'abbonato o dell'utente], con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che [i suoi dati di traffico siano utilizzati per scopi di marketing da parte di fornitori di servizi di comunicazione elettronica, oppure per la prestazione di uno specifico servizio a valore aggiunto].

La Direttiva e-Privacy prevede inoltre che il fornitore di servizi debba **informare** l'abbonato o l'utente dei servizi sul tipo di traffico dei dati oggetto del trattamento e sulla durata di tale trattamento; per il trattamento che si basa sul consenso (come abbiamo visto, per il marketing ed i servizi a valore aggiunto), l'informativa deve essere fornita ***prima dell'ottenimento del consenso*** (Art. 6(4)).

Infine, la Direttiva e-Privacy stabilisce che il trattamento dei dati del traffico da parte di un fornitore di servizi di comunicazione elettronica debba essere limitato ad una serie di **servizi**

---

[127] Alcuni siti prevedono periodi di conservazione di 25 anni, chiaramente eccedenti qualunque sia la finalità sottesa.

[128] Per i problemi relativi all'anonimizzazione, si veda la discussione nel contesto del RGPD nella Seconda Parte, sezione 2.1, *infra*.

sussidiari relativi alla fornitura del servizio (***fatturazione o gestione del traffico, indagini per conto dei clienti, accertamento delle frodi, commercializzazione dei servizi di comunicazione elettronica o prestazione di servizi a valore aggiunto)***, da parte di persone che agiscono sotto l'autorità del fornitore o sono al suo servizio, e **ristretto sulla base della "necessità di accesso"**: il trattamento deve essere limitato a quanto è strettamente necessario per lo svolgimento di tali attività (Art. 6(5)). Tuttavia, qualora necessario, "organismi [esterni] competenti", come quelli che si occupano della fatturazione o della risoluzione delle controversie attinenti alla fatturazione, si vedono comunque garantito il diritto di accesso ai dati sul traffico (Art. 6(6)).

La Direttiva e-Privacy è ancora più cogente nei riguardi del trattamento di "**dati relativi all'ubicazione diversi dai dati relativi al traffico**", vale a dire dati elaborati in una rete di comunicazione elettronica che indicano la ***posizione geografica dell'apparecchiatura terminale dell'utente*** (ed esempio, un cellulare) e che non sono trattati ***allo scopo di permettere una comunicazione elettronica o inviare una fatturazione per tale comunicazione***. Questi dati possono essere oggetto di trattamento solo quando vengono resi ***anonimi***,[129] oppure, se parliamo di ***servizi a valore aggiunto***, con il **consenso** degli utenti o degli abbonati a tali servizi (Art. 9(1), primo enunciato). Il fornitore di servizi di comunicazione elettronica ha, ancora una volta, l'obbligo di **informare** utenti e abbonati dei dettagli del trattamento, previo l'ottenimento del loro consenso (*idem*, secondo enunciato). L'utente e l'abbonato devono continuare ad avere la possibilità di negare, in ogni momento, il consenso (*idem*, terzo enunciato), e/o disconnetersi dal tracciamento dell'ubicazione, "mediante una funzione semplice e gratuita" (Art. 9(2)). Ancora una volta, il trattamento di tali dati è riservato alle persone che agiscono sotto l'autorità del fornitore del servizio di comunicazione elettronica o del terzo che fornisce il servizio a valore aggiunto (oppure al fornitore del servizio di uno dei due)(Art. 9(3)).

*NUOVO *Fatturazione dettagliata*

Gli abbonati hanno il diritto di ricevere **fatture non dettagliate** (Art. 7(1), e gli Stati membri devono anche applicare **modalità alternative che tutelino maggiormente la vita privata** in relazione a fatture dettagliate (Art. 7(2), ad es., fatture dettagliate che visualizzino solamente i prefissi nazionali o regionali per le chiamate in uscita, oppure escludano o oscurino le tre ultime cifre dei numeri chiamati, così da consentire sia di giustificare l'importo della fattura sia di tutelare la privacy dell'utente – che non necessariamente corrisponderà all'abbonato o a un componente il nucleo familiare).

*NUOVO *Presentazione e restrizione dell'identificazione della linea chiamante e collegata*

I fornitori di servizi di comunicazione elettronica devono garantire sia all'utente chiamante che all'utente chiamato (comprese le chiamate provenienti dall'UE [all'epoca CE] e dirette verso paesi terzi) **la possibilità di impedire l'identificazione della linea chiamante da parte dell'utente chiamato**; coloro che ricevono una chiamata da un numero sconosciuto (in provenienza dall' EU/CE o da un paese terzo) devono poter **bloccare** la chiamata e avere la possibilità di **impedire** l'identificazione della propria linea per ogni singola chiamata (Art. 8(1) – (4)).

[129] Si veda la nota precedente.

I fornitori di servizi di comunicazione elettronica devono, inoltre, **informare il pubblico** (e, naturalmente, i loro abbonati ed utenti) di tali possibilità (Art. 8(6)).

Nel rispetto delle legislazioni nazionali, e naturalmente dei principi generali di necessità e proporzionalità, i fornitori di servizi di comunicazione elettronica possono **annullare la soppressione** dell'identificazione della linea chiamante, o su richiesta dell'abbonato, ***per chiamate malintenzionate o inopportune***, cioè al fine di consentire accertamenti da parte dei fornitori e della polizia, e di acquisire elementi di prova in procedimenti giudiziari, o per gli organismi che trattano chiamate di emergenza (corpi di polizia, servizi di ambulanze e vigili del fuoco) ***perchè possano reagire a tali chiamate***(Art. 10(1) and (2)).

Ogni abbonato deve avere, inotre, "*la possibilità, gratuitamente e mediante una funzione semplice, di* ***bloccare il trasferimento automatico delle chiamate*** *verso il proprio terminale da parte di terzi*" (Art. 11).

Tutte le opzioni di cui sopra sono state tradotte in norme tecniche internazionali che oggi ne semplificano l'implementazione su smartphone ecc. .

*NUOVO *Elenchi di abbonati*

A seguito delle richieste delle autorità nazionali di protezione dati, la direttiva e-privacy incorpora disposizioni in base alle quali gli abbonati devono essere informati di ogni intenzione di includere i loro dati (per es, il numero del telefono di casa o del cellulare) in un **elenco abbonati,** sia a ***disposizione del pubblico,*** oppure ***ottenibile attraverso i servizi del fornitore***; devono inoltre godere del diritto a non essere inclusi in tali elenchi (cioè **"farsi togliere dall'elenco"**) senza onere alcuno e senza obblighi di motivazione (Art. 12(1) e (2)).

Si tratta di diritti che sono applicabili alle persone fisiche, anche se gli Stati membri devono assicurare che "*gli interessi legittimi degli abbonati che non siano persone fisiche*" [quindi gli interessi delle "persone giuridiche", come le aziende]" siano"sufficientemente tutelati" a tale riguardo (Art. 12(4)).

Se un elenco pubblico venisse utilizzato per "***scopi diversi … dalla ricerca di dati su persone*** *sulla base del loro nome e, ove necessario, di un numero minimo di altri elementi di identificazione*" – vale a dire se tali dati dovessero essere utilizzati per finalità di ***marketing diretto***, ***punteggi di affidabilità creditizia*** (***credit scoring)***[130] o ***campagne politiche*** – agli abbonati deve essere richiesto un **consenso ulteriore** riguardante l'utilizzo dei loro dati per tali finalità (Art. 12(3)).[131]

*NUOVO *Comunicazioni indesiderate*

Come sottolineato al punto 1.3.2, *supra*, la Direttiva sulla protezione dei dati del 1995 già

---

130 Cfr. il "**red-lining**": la prassi di applicare un trattamento differenziato per servizi quali la concessione di prestiti, alloggio, assicurazione e altri, basato sull'indirizzo di una persona e i dati storici dell'insolvenza della zona geografica in cui la persona dimora – una pratica dichiarata illegale negli USA molti anni fa. Si veda: https://www.investopedia.com/terms/r/redlining.asp
E inoltre: *How Redlining's Racist Effects Lasted for Decades*, NY Times, 24 agosto 2017, disponibile su: https://www.nytimes.com/2017/08/24/upshot/how-redlinings-racist-effects-lasted-for-decades.html (con cartine che illustrano questa pratica).

131 Non è chiaro se questo sia di applicazione anche alle "persone giuridiche", dal momento che questo paragrafo non è menzionato nel paragrafo 4 dell'Articolo 12, di cui sopra.

garantisce alle persone interessate il diritto incondizionato di **opporsi all'uso** di qualsiasi dato personale a scopo di marketing diretto (Art. 14(b) della Direttiva del 1995); per marketing si intende ogni tipo di marketing, di natura commerciale, politica o di altro genere. All'epoca, il riferimento era quasi esclusivamente al marketing postale. La Direttiva e-Privacy aggiunge una norma di **consenso previo** all'utilizzo di ***dispositivi automatici di chiamata*** e ***fax***[132] con tale scopo (Art. 13(1)). Il motivo è che l'invio di messaggi di marketing con questi dispositivi risulta molto meno costoso rispetto alla posta tradizionale, e quindi è più probabile che vi si faccia ricorso. Questa disposizione è di applicazione sia alle persone fisiche che a quelle giuridiche (singoli, individui, aziende ecc.). Inoltre, come già osservato nel paragrafo dedicato a "Obiettivi, finalità e ambito di applicazione della direttiva e-privacy", questa disposizione si applica a **qualunque soggetto** intenda utilizzare uno degli strumenti sopra ricordati per l'invio di messaggi di marketing diretto.

Tuttavia, se un cliente fornisce i propri dettagli di contatto elettronico (numero di telefono o indirizzo mail, ecc.) ad un'azienda nel contesto di una vendita di prodotti o servizi, il venditore ha il diritto di utilizzare tali dettagli per attività di **marketing di suoi prodotti o servizi simili** a questo cliente (il cosidetto "**marketing di prossimità**"), a condizione che al cliente sia offerta la possibilità di opporsi a tale offerta in ogni comunicazione (venga, cioè, offerto al cliente un "***opt-out***" da ulteriori attività di marketing in ciascuna comunicazione) (Art. 13(2)).

Per quanto riguarda altre tipologie di marketing diretto (ad es, il marketing diretto "non di prossimità" che utilizzi mezzi diversi dai fax o dai dispositivi automatici di chiamata), gli Stati membri possono **scegliere** fra il consenso previo ("***opt-in***" offerto al momento della raccolta dei dati personali) e il modello "***opt-out***" ("informato, non si è opposto")(Art. 13(3)).[133] In ogni caso, è vietata la prassi di inviare messaggi di posta elettronica a scopi di commercializzazione diretta "camuffando o celando l'identità del mittente da parte del quale la comunicazione è effettuata, o senza fornire un indirizzo valido cui il destinatario possa inviare una richiesta di cessazione di tali comunicazioni" (Art. 13(4)).

Deroghe

L'Articolo 15 della Direttiva e-Privacy stabilisce chiaramente che gli Stati membri possano limitare i diritti garantiti e gli obblighi imposti dalla Direttiva sulla stessa base della deroga, molto ampia, "**della salvaguardia di interessi pubblici rilevanti**", già figurante nella Direttiva sulla protezione dei dati del 1995 (Art. 13) e che recita: "*qualora tale restrizione costituisca una misura necessaria, appropriata e proporzionata in una società democratica, per la salvaguardia della* ***sicurezza nazionale*** *(ad es.* ***della sicurezza dello Stato****),* ***della difesa, della sicurezza pubblica, della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali***" – dettato cui la Direttiva e-Privacy si limita ad aggiungere: "o dell'***utilizzo non autorizzato dei sistemi di comunicazione elettronica***". Quanto enunciato viene ulteriormente rafforzato nella Direttiva e-Privacy che esplicitamente afferma che:

> "Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto

---

132 Una "macchina facsimile" o "fax" è uno strumento, utilizzato di rado ai nostri giorni, che permette l'invio di immagini (spesso quelle di un documento) attraverso una rete telefonica. Si veda: https://faxauthority.com/fax-history/

133 Il modello di "opt-out" dell'UE richiede che la persona interessata venga informata: (i) dell'intenzione di utilizzare i suoi dati per il marketing diretto; (ii) del diritto di opporsi a tale marketing; e (iii) dei dettagli sul come esercitare tale diritto (con mezzi semplici e senza oneri). Rileviamo che il modello europeo di "opt-out" differisce in modo sostanziale da quello degli U.S.A. che non obbliga all'informazione del soggetto interessato su tali aspetti.

> comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del Trattato sull'Unione europea".
>
> (Art. 15(1), ultima frase)

Gli articoli dei Trattati UE cui si fa qui riferimento si rifanno, rispettivamente, alla Carta dei diritti fondamentali dell'UE (annunciata nel 2000, in data quindi posteriore all'entrata in vigore della Direttiva sulla protezione dei dati del 1995) e alla Convenzione europea dei diritti dell'uomo.

Benché rappresenti un aperto riconoscimento del requisito (fondamentale e costitutivo dell'UE) del rispetto dei diritti e delle libertà fondamentali, non si tratta di qualcosa di nuovo: i principi e le norme di diritto figuravano già applicate nella prassi (e nella giurisprudenza) anche all'epoca della Direttiva "madre", come "Principi generali di diritto comunitario".[134]

L'Articolo 15(1), per la necessaria salvaguardia di "importanti interessi pubblici", di cui viene stilata una lista, pur sempre subordinati al *caveat* del rispetto dei diritti umani e dei principi generali del Diritto comunitario specifica anche che:

> "Gli Stati membri possono, *inter alia*, adottare misure legislatve che prevedano la **conservazione dei dati per un periodo limitato**, giustificate dai motivi enunciati nel presente paragrafo".
>
> (Articolo 15(1), secondo enunciato)

Il testo originale, nella sua **norma esplicita di limitazione del diritto**, con l'effettiva **proibizione di conservazione indiscriminata dei dati**, è importante alla luce dei successivi tentativi del legislatore europeo di imporre limitazioni proprio alla conservazione indiscriminata dei dati ai sensi della cosidetta Direttiva sulla conservazione dei dati, dichiarata nulla dalla Corte di Giustizia come vedremo al 1.3.4, *infra*.

Controllo e attuazione delle norme

Mentre l'attuazione della direttiva del 1995 è stata affidata ad autorità indipendenti per la protezione dei dati, e ciò vale anche per il RGPD, gli Stati membri avevano la possibilità di affidare le attività di controllo e attuazione delle disposizioni della direttiva e-privacy a un diverso soggetto, o a più soggetti. Si è quindi realizzata una diversa attribuzione dei compiti di controllo fra diverse autorità nei singoli Stati membri, in rapporto alle singole aree disciplinate dalla direttiva e-privacy.[135]

La Commissione ha rilevato che anche "l'attribuzione di competenze in materia di attuazione a un'ampia gamma di autorità, talora con margini di sovrapposizione" risultava aver "[ostacolato] l'efficacia delle norme in contesti transfrontalieri".[136]

Applicazione di altre norme fondamentali della Direttiva sulla protezione dei dati del 1995

---

134 Si veda la nota 67, *supra*.

135 Documento di lavoro della Commissione (nota 99, *supra*), Paragrafo 6.1.3, *Diversity of competent authorities*, p. 23. Per maggiori dettagli, si veda il lungo elenco di autorità competenti nei singoli Paesi membri con riguardo a compiti di controllo e attuazione di singole norme della Direttiva e-privacy (Allegato VI al Documento di lavoro della Commissione):

136 *Ibidem*.

In questa panoramica delle disposizioni della Direttiva e-Privacy va notato, infine, che tale Direttiva stabilisce chiaramente che i requisiti della Direttiva del 1995 in materia di **ricorsi giudiziali, responsabilità e sanzioni** (di cui abbiamo trattato alle sezione 1.3.2, *supra*) si applichino anche in relazione alla Direttiva e-Privacy (Art. 15(2)); che il **Gruppo di lavoro Articolo 29** (trattato nella stessa sezione) svolga i compiti fissati della Direttiva del 1995 anche per quanto concerne le materie disciplinate dalla Direttiva e-Privacy (Art. 15(3)); infine, che gli Stati membri devono prevedere sanzioni "effettive, proporzionate e dissuasive" per le violazioni della Direttiva (Art. 15-bis).

1.3.4 Strumenti di protezione dati nell'ambito del Terzo pilastro[137]

Nel periodo compreso fra la metà degli anni '90 dello scorso secolo e il 2009, l'Unione europea ha creato un numero consistente di organismi deputati a facilitare la cooperazione fra gli Stati membri nell'area del diritto penale e della sicurezza pubblica ("Giustizia e affari interni", o GAI), il cosiddetto "Terzo pilastro" dell'Ue.[138] Tutti questi organismi trovavano la loro ragion d'essere nella costituzione di database paneuropei contenenti informazioni personali e nelle norme e procedure finalizzate a consentire l'accesso a tali database e lo scambio di dati personali fra gli Stati membri.

Si tratta del'Europol (1998), del Sistema d'informazione Schengen (SIS-I, 2001, poi trasformato in SIS-II nel 2013), dell'Eurojust (2002), dell'Eurodac (2003), del Sistema d'informazione visti (VIS, 2004) e del Sistema d'informazione doganale (CIS, 2009).

Durante tale periodo, il Consiglio Ue ha adottato ben 123 strumenti di varia natura nell'area GAI.[139] Nel 2005 è stata firmata da sette Stati membri la Convenzione di Prüm, e con la decisione adottata il 23 giugno 2008 il Consiglio europeo stabilì di integrarne le principali disposizioni nel quadro giuridico dell'Ue al fine di consentire più ampi scambi di dati biometrici (DNA e impronte digitali) fra tutti gli Stati membri dell'Ue ai fini del contrasto al terrorismo e alla criminalità transfrontaliera.

Nel 2008 il Consiglio ha quindi adottato una Decisione quadro di portata generale con cui venivano definiti principi comuni per la tutela dei dati personali nel settore GAI.[140] Tuttavia, anche se numerose delle norme contenute in tale Decisione quadro traevano ispirazione da quelle della direttiva 95/46/CE e dalla Convenzione del Consiglio d'Europa, come osservava l'allora Garante europeo della protezione dei dati, Peter Hustinx, "il livello di protezione era

---

[137] Per approfondimenti sulla normativa di settore, si vedano i paragrafi relativi alla storia normativa nei rispettivi capitoli all'interno di Steve Peers, (2016). EU Justice and Home Affairs Law: Volume I: EU Immigration and Asylum Law (Fourth Edition) and Volume II: EU Criminal Law, Policing, and Civil Law (Fourth Edition), both Oxford University Press, 2016.

[138] V. nota 67, *supra*.

[139] V. Emilio De Capitani, Metamorphosis of the third pillar: The end of the transition period for EU criminal and policing law, *EU Law Analysis blogspot*, 10 July 2014, consultabile qui: https://eulawanalysis.blogspot.com/2014/07/metamorphosis-of-third-pillar-end-of.html

[140] Decisione quadro del Consiglio 2008/977/GAI del 27 novembre 2008 sulla protezione dei dati personali trattati nel quadro della cooperazione di polizia e giudiziaria in materia penale, disponibile qui: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008F0977

molto inferiore in termini di portata e di sostanza."[141] Quanto alla portata della decisione, Hustinx faceva notare che:[142]

> la Decisione si applica esclusivamente qualora dati personali siano trasmessi a o messi a disposizione di altri Stati membri, per cui non ricomprende anche i trattamenti "nazionali" [ossia, i trattamenti svolti da uno Stato membro sul proprio territorio], a differenza della direttiva 95/46/CE.

Nel 2009, a seguito dell'entrata in vigore del Trattato di Lisbona che pose fine alla struttura tripartita in pilastri[143], ebbe inizio un periodo transitorio quinquennale durante il quale la normativa Ue nel settore GAI avrebbe dovuto essere allineata ai principi giuridici di rango costituzionale vigenti nell'Ue (v. paragrafo 1.4.2, *infra*)[144]. Nel 2018, la Decisione quadro è stata sostituita da una nuova Decisione (*idem*).

1.3.5. La protezione dei dati nel Secondo pilastro

Fra il 1970 e il 1993 ha operato un sistema informale di "Cooperazione politica europea" (CPE) nelle materie esterne. Con il Trattato di Maastricht, entrato in vigore alla fine del 1993, si passò alla formalizzazione di una "Politica estera e di sicurezza comune" (PESC), il "secondo pilastro" dell'Ue. Tuttavia, fino all'ulteriore evoluzione della PESC dovuta al Trattato di Lisbona del 2009 (che ha abolito la struttura a pilastri)[145], come meglio illustrato nel paragrafo 1.4.4. *infra*, non vi erano norme specifiche di protezione dei dati applicabili al trattamento di dati personali in questo ambito (a eccezione delle norme vigenti nei singoli Stati membri e della Convenzione del Consiglio d'Europa).

1.3.6. La protezione dei dati per le istituzioni dell'Ue

Fino al 2001 non vi erano norme specifiche né un corpus coerente di norme in materia di protezione dei dati per quanto riguardava le istituzioni dell'Ue in quanto tali. In quell'anno fu un regolamento (il Regolamento (CE) 45/2001) a introdurre per la prima volta disposizioni specifiche in materia, sul fondamento dell'Articolo 286 del TUE che imponeva l'esistenza di norme all'uopo.[146]

Le disposizioni sulla protezione dei dati contenute nel Regolamento del 2001 si basavano sulle norme comunitarie all'epoca vigenti in questo ambito, come applicate dagli Stati membri, e

---

[141] Peter Hustinx, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, p. 15, disponibile qui: https://www.statewatch.org/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf

[142] Idem, con riguardo al considerando 7 e all'art. 1 della Decisione quadro.

[143] V. nota 67, *supra*.

[144] Si veda il Protocollo 36 al Trattato di Lisbona, e l'articolo citato di Emilio De Capitani (nota 167, *supra*).

[145] V. nota 67, *supra*.

[146] Regolamento (CE) 45/2001 del Parlamento europeo e del Consiglio del 18 dicembre 2000 sulla protezione delle persone fisiche con riguardo al trattamento di dati personali da parte delle istituzioni e degli organismi della Comunità e sulla libera circolazione di tali dati, consultabile qui: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32001R0045

in particolare sulla direttiva del 1995 e sulla direttiva del 2002 in materia di e-privacy.

Il Regolamento 45/2001 prevedeva anche l'istituzione del Garante europeo per la protezione dei dati quale autorità di controllo indipendente incaricata di vigilare sul trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, e imponeva a ciascuna di tali istituzioni di designare un Responsabile della protezione dei dati (RPD).

Il Regolamento (CE) 45/2001 è stato abrogato dal Regolamento (UE) 2018/1725, entrato in vigore l'11 dicembre 2018; sul punto, v. il paragrafo 1.4.5 *infra*.

1.4 La normativa sulla protezione dei dati nel futuro

Alla fine del primo decennio del XXI sec. è emerso chiaramente che gli strumenti fondamentali di protezione dei dati del XX sec., di cui abbiamo parlato nella sezione 1.3, *supra*, non erano più sufficienti: erano stati concepiti e redatti prima del massiccio accesso a Internet (o, quanto meno, al world-wide web), a dispositivi di controllo incorporati con diffusione delle capacità di elaborazione nell'ambiente ("ubiquitous computing"), a dispositivi mobili, "Big Data", l'"Internet degli oggetti" (IoT), profilazioni approfondite, processi decisionali algoritmici e "Intelligenza Artificiale" (AI). Sia a livello del Consiglio d'Europa che dell'UE, vennero allora elaborati nuovi o "aggiornati" strumenti di protezione di cui ci accingiamo a parlare in questa sezione.

1.4.1 Il Regolamento generale sulla protezione dei dati dell'UE

La Commissione Europea ha proposto l'adozione di un Regolamento generale sulla protezione dei dati (RGPD) nel 2012,[147] per rispondere alle sfide lanciate dalle nuove tecnologie e dai servizi annessi. Fu subito chiaro che sarebbe stato necessario un livello forte ed elevato di protezione dei dati come *conditio sine qua non* per creare un clima di fiducia nell'ambiente online che in sé costituisce un "*fattore chiave dello sviluppo economico*"; il nuovo, aggiornato regime di protezione dei dati ai sensi della *lex generalis* avrebbe giocato un ruolo "*centrale nell'Agenda digitale europea e, più in generale, nella Stategia Europa 2020*".[148]

Il contesto, lo statuto, l'approccio e gli elementi chiave del RGPD sono descritti in dettaglio nella seconda Parte di questo Manuale. Qui è sufficiente notare che il RGPD **amplia e rafforza**

147 Proposta di Regolamento del Parlamento Europeo e del Consiglio relativa alla protezione degli individui in relazione al trattamento dei dati personali e allla libera circolazione di tali dati (Regolamento generale sulla protezione dei dati), COM(2012) 11 finale, Bruxelles, 25.01.2012, disponibile su: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN
Contemporaneamente, la Commissione ha anche proposto uno strumento di protezione dei dati separato, una Proposta di Direttiva "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", (COM(2012) 10 finale), Direttiva che non viene analizzata in questo Manuale (si veda la nota nel riquadro intitolato "*Il Manuale*", a pagina 1 del Manuale).

148 Proposta per un RGPD (nota precedente), pp. 1 – 2 (con riferimenti ai documenti principali sull'Agenda Digitale e sulla Strategia Europa 2020). All'Agenda Digitale succede la Strategia del Mercato unico digitale ("DSM Strategy").

significativamente le disposizioni e le norme principali; **aggiunge espressamente i dati genetici e biometrici al catalogo dei dati "sensibili"** (sulla base del lavoro condotto sulla versione "modernizzata" della Convenzione del Consiglio d'Europa in materia di protezione dati, v. *infra*, 1.4.3); è finalizzato ad una **maggiore armonizzazione** della legislazione sulla protezione dei dati negli Stati membri dell'UE (almeno negli ambiti di applicazione che, in senso lato, sono ancora una volta quelli che, in passato, costituivano il "Primo Pilastro" delle Comunità Europee), in linea con la nuova giurisprudenza della Corte di Giustizia – anche se è soggetto ad un ventaglio di ***"clausole di specificazione"*** (ossia, disposizioni che lasciano al diritto nazionale degli Stati membri la disciplina più particolareggiata di alcune materie, entro il quadro complessivamente offerto dal RGPD, dai trattati Ue come interpretati dalla Corte di giustizia dell'Ue, e dai principi costituzionali nonché dai sistemi giuridici dei singoli Stati)[149]; stabilisce **diritti più forti (e in alcuni casi nuovi) per i soggetti interessati**; favorisce una **cooperazione transfrontaliera molto più stretta** fra le DPA degli Stati membri e dovrebbe comportare una **migliore e più coerente applicazione e osservanza delle norme**.

Più nel dettaglio, come già rilevato nell'Introduzione di questo Manuale, il RGPD introduce (o quantomeno rende molto più specifico) **il "principio di responsabilizzazione" – ora fondamentale e obbligatorio in tutti gli Stati membri –**, e in molti casi (anche alle autorità pubbliche subordinate al regolamento) ***obbliga*** alla creazione e alla nomina (da parte di titolari o responsabili) di un **Responsabile della protezione dei dati** (**RPD**).

Come avremo modo di spiegare nella seconda Parte, i due elementi sono collegati: in base al RGPD, i RPD saranno coloro che, nella pratica, dovranno garantire il rispetto del principio di responsabilizzazione da parte delle, e nelle organizzazioni per le quali lavorano.

1.4.2 La proposta di Regolamento UE sulla e-Privacy

Sebbene, come rilevato nella precedente sotto-sezione, uno degli scopi principali della proposta di un RGPD fosse quello di rispondere alle sfide legate alla **mancanza di fiducia (in particolare, quella dei consumatori) nell'ambiente online**, alla Commissione ci vollero altri cinque anni per proporre un nuovo strumento che sostituisse le norme più rilevanti in materia, come quelle della Direttiva e-Privacy (Direttiva 2002/58/CE), di cui abbiamo parlato alla sezione 1.3.4, *supra* (che rimane comunque in vigore anche nel suo statuto di "orfana").

Il nuovo testo ha preso la forma di una proposta presentata nel gennaio 2017, destinata a sostituire anche la Direttiva e-Privacy con un Regolamento, **la proposta di Regolamento e-Privacy**.[150]

La proposta è ancora in una fase iniziale dell'iter legislativo: al momento della stesura di questo testo (dicembre 2018), era ancora in fase di discussione interna al Consiglio e oggetto di grande attenzione sia da parte dei fautori (Gruppi per le libertà civili, consumatori e Gruppi per i diritti al digitale)[151] che dei detrattori (comprese alcuni dei maggiori "Giganti di Internet"

---

[149] Si veda la Parte II, paragrafo 2.2., *infra*, alla voce "… ma con "clausole di specificazione" ".

[150] Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), COM(2017) 10 finale, Bruxelles, 10.01.2017: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN

[151] Si veda la Lettera aperta agli Stati membri sulla riforma della ePrivacy, firmata da un gran numero di ONG il 27 marzo 2018 e consultabile su: https://edri.org/files/eprivacy/20180327-ePrivacy-openletter-final.pdf

statunitensi, che chiedono la revoca completa della proposta o una sua significativa edulcorazione).[152] Per questi motivi è prematuro discutere nel dettaglio della proposta di Regolamento: è indubbio che la versione finale sarà alquanto diversa dalla proposta, almeno sotto alcuni aspetti.

Per questa prima edizione del Manuale è sufficiente presentare i **punti chiave della proposta della Commissione**, come elaborati dalla Commissione stessa:[153]

> La proposta per un Regolamento in materia di norme di alto livello riguardanti la privacy per tutte le comunicazioni elettroniche include:
>
> - **Nuovi attori:** le norme sulla privacy [*e la protezione dei dati*] si applicheranno, in futuro, anche ai nuovi attori [i cosidetti *"Over-The-Top" o OTT*], fornitori di servizi di comunicazione elettronica come WhatsApp, Facebook, Messenger e Skype. Lo scopo è quello di fare in modo che questi servizi, molto popolari, garantiscano lo stesso livello di riservatezza delle comunicazioni di quello offerto dai tradizionali operatori di telefonia.
> - **Regole più rigide:** con questo Regolamento, di diretta applicazione, tutti i cittadini e le imprese dell'UE godranno dello stesso elevato livello di protezione delle loro comunicazioni elettroniche. Le imprese, inoltre, beneficieranno di un'unica serie di norme in tutta la UE.[154]
> - **Contenuto delle comunicazioni e metadati:** è garantita la privacy sia per il contenuto delle comunicazioni sia per i metadati, come ad esempio ora della chiamata e ubicazione. I metadati presentano un'alta componente di privacy e devono essere resi anonimi o cancellati qualora gli interessati neghino il consenso, a meno che i dati siano necessari per le fatturazioni.[155]
> - **Nuove opportunità per gli operatori:** una volta accordato il consenso per il trattamento dei dati delle comunicazioni e/o i metadati, gli operatori tradizionali di telecomunicazioni godranno di maggiori opportunità per la fornitura di servizi aggiuntivi e lo sviluppo aziendale. Potranno, per esempio, produrre mappe termiche per indicare la presenza di persone, uno strumento che potrebbe favorire lo sviluppo di nuovi progetti infrastrutturali da parte delle autorità pubbliche e delle aziende di trasporto.

---

[152] Si veda: Corporate Europe Observatory, *Shutting down ePrivacy: lobby bandwagon targets Council*, 4 giugno 2018, disponibile su: https://corporateeurope.org/power-lobbies/2018/06/shutting-down-eprivacy-lobby-bandwagon-targets-council

[153] https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation (grassetto in originale, parole in virgolettato, corsivi e note aggiunte)

[154] Sottolineiamo che questo dipenderà dalle disposizioni del regolamento e-Privacy prive di "clausole di flessibilità"/ "clausole di specificazione" come quelle che figurano nel RGPD (si veda la Seconda Parte, sezione 2.1, *infra*). Se il testo finale del regolamento e-Privacy dovesse contenere norme così "flessibili" (come molto probabile), sarebbe di fondamentale importanza l'aggiunta, soprattutto per l'ambiente online, per sua intrinseca natura transnazionale, di una norma di "diritto applicabile".

[155] Vanno sottolineati i continui tentativi da parte degli Stati membri e della Commissione di mantenere o reintrodurre la conservazione obbligatoria dei (meta-)dati di comunicazione elettronica: si veda la sezione 1.3.4, *supra*.

- **Norme semplificate per i cookie:** la previsione sui cookie, che ha generato un sovraccarico di richieste di consenso per gli utenti di internet, verrà razionalizzata. La nuova norma permetterà un uso più agevole grazie alle impostazioni dei browser che semplificheranno le procedure di accettazione o rifiuto di cookie di monitoraggio e altri identificatori. La proposta chiarisce, inoltre, che il consenso non è richiesto per i cookie non invasivi della privacy e che migliorano l'esperienza dell'utente (ad es. lo storico del carrello elettronico della spesa) oppure per quelli utilizzati da un sito web nel conteggio del numero di visitatori.
- **Protezione anti spam:** la proposta vieta le comunicazioni elettroniche indesiderate via e-mail, SMS e sistemi automatizzati di chiamata. *In funzione del diritto nazionale,* gli interessati saranno tutelati per default (cioè per impostazione predefinita) o potranno figurare in un "registro delle opposizioni" (do-not-call list) per non ricevere telefonate a fini di marketing.[156] Gli operatori di marketing dovranno garantire la visualizzazione del numero di telefono chiamante o utilizzare un prefisso speciale che identifichi una chiamata di marketing.
- **Applicazione della norma più efficace:** l'applicazione delle norme sulla riservatezza previste dal Regolamento sarà affidata alle autorità di protezione dei dati, che già vigilano sull'applicazione delle disposizioni del Regolamento generale sulla protezione dei dati (RGPD).

1.4.3 La Direttiva del 2016 sulla protezione dei dati nelle attività giudiziarie e di polizia (DPDPG)

L'articolo 10, paragrafo 1, del Protocollo 36 al Trattato di Lisbona del 2009 prevedeva un periodo transitorio prima della piena applicazione dei poteri della Commissione e della Corte di giustizia agli atti giuridici dell'Ue nel settore della cooperazione di polizia e giudiziaria in materia penale adottati precedentemente all'entrata in vigore del Trattato stesso (il cosiddetto "acquis del Terzo pilastro"). Tale periodo transitorio ha avuto termine il 1 dicembre 2014.

Nel 2012, la Commissione ha presentato la proposta di una direttiva in questo ambito unitamente alla proposta di un Regolamento generale sulla protezione dei dati (cui si è fatto cenno nel paragrafo 1.4.1, *supra*, e al quale saranno dedicati approfondimenti nella Parte II del Manuale).[157] Tuttavia, analogamente al RGPD, la Direttiva sulla protezione dei dati nelle attività giudiziarie e di polizia (DPDPG, anche nota come

[156] Questo è un esempio evidente di "clausola di specificazione" di cui abbiamo parlato nel paragrafo 1.3.3., *supra*, alla voce "Complicazioni" – che ben illustra la necessità di una norma sul "diritto applicabile" che chiarisca quale della varie norme nazionali siano di applicazione nel caso di corrispondenza transfrontaliera a fini di marketing.

[157] V. nota 149, *supra*.

"direttiva polizia e giustizia") è stata adottata solo nel 2016, in pari data al RGPD.[158] A differenza del RGPD, che in quanto regolamento è in linea di principio direttamente applicabile nel sistema giuridico di tutti gli Stati membri (anche se contiene un numero significativo di clausole che, nei fatti, necessitano di ulteriori "specificazioni" da parte del diritto interno)[159], la DPDPG, in quanto direttiva, non è di diretta applicazione (ossia, non esplica un "effetto diretto") necessitando di un **recepimento** nel diritto interno. Tale recepimento avrebbe dovuto aver luogo entro due anni dall'entrata in vigore della direttiva, ossia entro il 6 maggio 2018 (poche settimane prima dell'applicazione effettiva del RGPD, il 25 maggio dello stesso anno).

Si osservino, tuttavia, i più ampi termini di implementazione previsti dagli articoli 61-63 della direttiva, legati a molteplici circostanze riferite all'enorme numero di trattamenti coinvolti, e dei quali parleremo sinteticamente al termine di questo paragrafo dedicato alla DPDPG alla voce "Recepimento ritardato".

Per adesso è sufficiente rilevare i tratti salienti e i principali obblighi previsti dalla DPDPG.

Una direttiva anziché una decisione-quadro del Consiglio

Una prima considerazione si impone, ossia che l'aver fissato le norme sul trattamento di dati personali in una direttiva costituisce di per sé **un passo avanti significativo** rispetto al prevedere tali norme in una decisione-quadro del Consiglio come quella del 2008 (che la DPDPG ha abrogato)[160]. Trattandosi di una direttiva, è infatti possibile invocarne l'applicazione direttamente da parte dei singoli dinanzi alle corti nazionali (e, in ultima istanza, anche dinanzi alla Corte di giustizia), e la sua applicazione è soggetta ai poteri di verifica della Commissione che mirano a garantire la corretta transposizione nel diritto interno di ogni strumento di questo tipo.

Ambito di applicazione della DPDGP

i. Ambito oggettivo di applicazione della direttiva

Quanto al suo ambito di applicazione, la DPDGP recita:

1. La presente direttiva si applica al trattamento dei dati personali da parte delle autorità competenti per le finalità di cui all'articolo 1, paragrafo 1 [a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia

[158] 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, disponibile qui: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ITA. La direttiva è entrata formalmente in vigore il giorno successivo alla sua pubblicazione nella Gazzetta ufficiale (cioè il 5 maggio 2016), ma come rilevato nel paragrafo, il termine effettivo per la sua applicazione (previo recepimento nel diritto interno degli Stati membri) era fissato a due anni da tale data, ossia entro il 6 maggio 2018.

[159] V. Parte II, Sezione 2.2. *infra*.

[160] Si veda Steve Peers, *The Directive on data protection and law enforcement: A Missed Opportunity?*, Statewatch Analysis blog, April 2012, consultabile qui: https://www.statewatch.org/analyses/no-176-leas-data%20protection.pdf

contro e la prevenzione di minacce alla sicurezza pubblica].

2. La presente direttiva si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

3. La presente direttiva non si applica ai trattamenti di dati personali:

a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;

b) effettuati da istituzioni, organi, uffici e agenzie dell'Unione.

La specifica linea di confine che, all'interno di ogni "autorità competente", separa i trattamenti soggetti alla direttiva da quelli soggetti al RGPD dovrà essere tracciata tenendo conto del considerando (12) della direttiva stessa. Quest'ultimo chiarisce, all'ultimo periodo, che il trattamento di dati personali relativo ad "altri compiti" conferiti alle "autorità competenti" e "che non siano necessariamente svolti a fini di prevenzione, indagine, accertamento o perseguimento di reati, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica," è soggetto al RGPD anziché alla DPDPG.

Il titolare dovrà quindi porre particolare attenzione a tale linea di confine, nonché ad altre questioni fra cui l'applicabilità della DPDPG alla raccolta e all'ulteriore trattamento di dati personali in rapporto a "incidenti" ove non sia chiaro, nell'immediato, se si configurino reati, ovvero in rapporto all'adozione di misure (comprese "misure coercitive") in occasione di manifestazioni o grandi eventi sportivi che "possono dar luogo a reati". Le risposte fornite a tali interrogativi comportano effetti sostanziali in termini di livello di protezione dei dati da garantire – per esempio, in termini di informativa agli interessati, limiti al periodo di conservazione dei dati, limiti ai diritti degli interessati, ecc. . Nel frattempo, i responsabili della protezione dei dati che operano presso le autorità competenti dovranno assistere queste ultime nel compiere le scelte necessarie così da garantire in ogni caso il livello adeguato di protezione.

Il concetto di "**sicurezza pubblica**" trova generalmente applicazione in riferimento a eventuali deroghe al diritto Ue, ossia per segnalare circostanze che giustificano attività altrimenti in violazione del diritto Ue. Come rilevato da Koutrakis, "la sicurezza pubblica rappresenta il fondamento di deroghe a tutte e quattro le libertà fondamentali dell'Unione".[161] Per citare una Nota informativa predisposta su richiesta della Commissione IMCO presso il Parlamento europeo,[162]

[161] Panos Koutrakis, *Public Security Exceptions and EU Free Movement Law*, in: Koutrakos, P., Nic Shuibhne, N. and Sypris, P. (Eds.), Exceptions from EU Free Movement Law, 2016 (pp. 190-217), p.2, disponibile qui: http://openaccess.city.ac.uk/16192/
(Con riguardo agli artt. 36 (Beni), 45(3) e 52 (Persone), 62 (Servizi), e 65 TFUE (Capitali)).

[162] Public Security Exception in the Area of non-personal Data in the European Union, Briefing Paper requested by the IMCO Committee of the European Parliament and prepared by Kristina Irion, PE 618.986, April 2018, p. 3, disponibile qui:
https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/618986/IPOL_BRI(2018)618986_EN.pdf

> Fra tutte le motivazioni poste a fondamento di deroghe alla libertà di circolazione, la sicurezza pubblica presenta la più stretta correlazione con quello che costituisce tradizionalmente il nucleo forte della sovranità nazionale, ossia quelle attività in cui è allo Stato che spetta in prima battuta il compito di tutelare il proprio territorio e i cittadini che vi si trovano.

La giurisprudenza della CGUE in materia di "sicurezza pubblica" si incardina sulla sentenza nel caso Campus Oil[163], in cui la Corte ha ritenuto giustificata una misura nazionale (nello specifico, la fissazione di una quota nazionale per la fornitura di combustibili nella Repubblica d'Irlanda) in quanto i combustibili dovevano considerarsi

> "**essenziali per l'esistenza di uno stato** poiché da loro dipendono il funzionamento non solo dell'economia, ma soprattutto delle istituzioni e dei servizi pubblici essenziali, e perfino la sopravvivenza della popolazione." (paragrafo 34)

Ciò chiarisce, da un lato, che il termine "sicurezza pubblica" nell'accezione accolta nel diritto Ue non si limita alle materie di natura penale, bensì comprende anche materie quali la tutela di "servizi pubblici essenziali" e misure intese ad assicurare "la sopravvivenza della popolazione"; d'altro canto, ne consegue che l'ambito della "sicurezza pubblica" non coincide con quello di "ordine pubblico", termine di utilizzo frequente nella normativa concernente le attività di polizia con riguardo ad attività quali il mantenimento dell'ordine in occasione di manifestazioni, parate ed eventi analoghi.[164] In effetti, come evidenziato dal Consiglio, l'oggetto meritevole di tutela deve riguardare:[165]

> una minaccia reale e sufficientemente grave nei confronti di uno degli interessi fondamentali della società, quale una minaccia al funzionamento di istituzioni e servizi pubblici essenziali e alla sopravvivenza della popolazione, ovvero il rischio di un grave turbamento delle relazioni internazionali o della coesistenza pacifica degli Stati, o un rischio per interessi di natura militare.

Stabilire con precisione l'ambito delle minacce (di natura penale?) per la "sicurezza pubblica" comporta numerose difficoltà in alcune circostanze specifiche. In quali casi, per esempio, disordini publici quali quelli causati dall'interruzione dei voli a opera di manifestanti contro l'espulsione forzata di richiedenti asilo configurano una "minaccia a un servizio pubblico essenziale"?[166] E in quali casi il rischio di "turbamento delle relazioni internazionali" (per esempio una manifestazione contro la visita ufficiale di un capo di stato) è sufficientemente grave da configurare un rischio per la sicurezza

---

[163] Sentenza nella Corte del 10 luglio 1984, *Campus Oil Limited and others v Minister for Industry and Energy and others*, Caso 72/83, ECR 1984 -02727, disponibile qui: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:61983CJ0072&from=IT

[164] Si veda, per esempio, http://www.lokalepolitie.be/5371/contact/diensten/20-handhaving-openbare-orde (in olandese)

[165] Council of the European Union, Interinstitutional File: 2017/0228 (COD), Recital (12a), p.3 , disponibile qui: http://www.consilium.europa.eu/media/32307/st15724-re01en17.pdf

[166] Nel Regno Unito si è discusso a lungo in merito al procedimento e alla condanna comminata nei confronti di manifestanti del tipo qui descritto ai sensi della normativa sul contrasto al terrorismo (ossia, ai sensi di norme attinenti alla "sicurezza pubblica") anziché sulla base delle norme penali ordinarie in materia di violazione della proprietà privata. Sul caso pende una richiesta di appello. Si veda: https://www.theguardian.com/global/2019/feb/06/stansted-15-rights-campaigners-urge-judge-to-show-leniency

pubblica? E tuttavia, dalla risposta a questi interrogativi dipende l'applicabilità della direttiva polizia e giustizia ai trattamenti di dati personali svolti in rapporto a eventi del genere.

Se è vero che a molti soggetti, soprattutto in ambito pubblico come gli enti locali o le agenzie per la tutela dell'ambiente, gli enti assistenziali o gli organismi per la tutela degli animali, sono stati conferiti alcuni poteri di natura autoritativa con riguardo a (determinati) reati e minacce per la sicurezza pubblica, è pur vero che i compiti primari di tali soggetti non sono connessi all'indagine ecc. di reati commessi nei rispettivi ambiti, né alle minacce all'ordine pubblico (collegate o meno a reati).

I RPD operanti presso tali enti o soggetti pubblici dovranno valutare attentamente in quale misura i trattamenti di dati personali svolti dagli enti e soggetti in questione siano da considerarsi disciplinati dal RGPD ovvero dalla DPDPG. Molto spesso non sarà facile identificare immediatamente l'approccio corretto, e il RPD dovrà quindi approfondire la questione con l'aiuto del titolare, del servizio giuridico competente e dell'autorità di controllo nazionale. Inoltre, i dati personali oggetto di trattamenti che sono disciplinati dalla DPDPG dovranno essere tenuti separati, in via generale, da quelli trattati secondo le regole del RGPD, e si dovranno prevedere regole e procedure specifiche per i casi in cui dati appartenenti a una categoria/trattati per un determinato scopo potranno essere utilizzati secondo le regole proprie dell'altra categoria ovvero per uno scopo diverso.[167]

Vi è, infine, da considerare la tematica della delimitazione fra, da un lato, le attività degli Stati membri dell'Ue nel settore della "prevenzione, indagine, accertamento o perseguimento di reati" e della "salvaguardia contro e prevenzione di minacce alla sicurezza pubblica" e, dall'altro lato, le attività svolte dagli Stati membri e dalle rispettive agenzie o unità in materia di sicurezza nazionale. I confini fra questi due ambiti di attività, dei quali il primo ricade teoricamente nel diritto unionale, mentre il secondo ne esula totalmente, sono sempre più incerti – soprattutto alla luce della incerta categorizzazione di "terrorismo", "criminalità informatica", "sicurezza informatica", ecc. .[168]. In realtà, [169]

> In alcuni Paesi, si assiste a una crescente ibridazione fra agenzie competenti, che operano sia ai fini del contrasto alla criminalità sia ai fini della tutela della sicurezza

[167] Si veda anche l'analisi condotta nel paragrafo 1.4.6, *infra*, sui flussi di dati personali fra soggetti diversi operanti alla luce dei diversi regimi giuridici vigenti nell'Ue.

[168] Douwe Korff, Ben Wagner, Julia Powles, Renata Avila e Ulf Buermeyer, Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes, comparative report covering Colombia, DR Congo, Egypt, France, Germany, India, Kenya, Myanmar, Pakistan, Russia, South Africa, Turkey, UK, USA, redatto per la World Wide Web Foundation, gennaio 2017, in particolare v. par. 2.3.1, disponibile qui: https://ssrn.com/abstract=2894490

[169] Idem, p. 27. L'espansione in chiave "preventiva" del ruolo svolto dalla polizia non è cosa nuova. Si veda Ian Brown & Douwe Korff, Privacy & Law Enforcement, FIPR study for the UK Information Commissioner, 2005, Paper No. 4, The legal framework, section 3.1. Per gli sviluppi più recenti, anche in rapporto alla incerta delimitazione fra attività di polizia e attività connesse alla sicurezza nazionale, si veda Douwe Korff, Protecting the right to privacy in the fight against terrorism, Issue Paper written for the Commissioner for Human Rights of the Council of Europe, 2008, disponibile qui: https://wcd.coe.int/ViewDoc.jsp?Ref=CommDH/IssuePaper(2008)3.

nazionale. L'FBI degli USA ne rappresenta l'esempio principe[170], ma anche nel Regno Unito l'agenzia per la sicurezza nazionale (GCHQ) lavora sempre più in stretto rapporto con le autorità di polizia.[171]

Non è questa la sede per un'analisi approfondita del tema, che sarà comunque toccato brevemente nell'ambito del paragrafo 1.4.6., relativo alla trasmissione di dati personali da un titolare soggetto a una determinata legislazione in materia di protezione dei dati nell'Ue verso un altro titolare soggetto a un diverso corpus di norme Ue in materia – ovvero, nel caso di agenzie per la sicurezza nazionale, sottratto all'applicazione del diritto Ue.

D'altro canto, la distinzione fra trattamenti di dati personali disciplinati dalla direttiva e trattamenti di dati personali da parte delle istituzioni, degli organi e delle agenzie dell'Unione è inequivocabile, essendo questi ultimi disciplinati dal nuovo regolamento adottato nel 2018 (v. paragrafo 1.4.6, *infra*).

ii. Ambito soggettivo di applicazione

Anche rispetto all'ambito soggettivo di applicazione, la direttiva polizia e giustizia definisce come segue le "autorità competenti" di cui all'Articolo 1, paragrafo 1:

> a) qualsiasi autorità pubblica competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; o
>
> b) qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica;
>
> (v. Art. 3, paragrafo 7)

Si è già rilevato che tale ambito soggettivo può comprendere soggetti ben diversi dalla

[170] Nella pagina sul sito dell'FBI dedicata alla "Gestione delle minacce alla sicurezza informatica della nazione" si afferma esplicitamente che l'FBI ha il compito di tutelare la sicurezza nazionale degli USA e di operare quale principale forza di polizia del paese e, inoltre, che "tali ruoli sono complementari, poiché le minacce alla sicurezza informatica della nazione possono provenire da altre nazioni, da organizzazioni terroristiche, e da organizzazioni criminali transnazionali, e non sempre le rispettive demarcazioni sono facili da individuare.". Si veda: www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity . Di recente l'FBI ha modificato i contenuti di una scheda informativa indicando che la sua "funzione primaria" non consiste più nella "applicazione della legge" ma nella "sicurezza nazionale". Si veda: The Cable, 5 January 2014, disponibile qui: http://thecable.foreignpolicy.com/posts/2014/01/05/fbi_drops_law_enforcement_as_primary_mission#sthash.4DrWhlRV.dpbs. Su rischi connessi alla commistione fra i vari ambiti, si veda www.foreignpolicy.com/articles/2013/11/21/the_obscure_fbi_team_that_does_the_nsa_dirty_work [Nota originale].

[171] Si veda : Computer Weekly, "*GCHQ and NCA join forces to police dark web*", 9 Nov 2015: http://www.computerweekly.com/news/4500257028/GCHQ-and-NCA-join-forces-to-police-dark-web [Nota originale].

polizia e da altri organismi delle forze dell'ordine, in base all'impalcatura costituzionale dei singoli Paesi: enti pubblici locali e regionali, agenzie sanitarie e di welfare, organismi di vigilanza delle istituzioni finanziarie o dell'ambiente, agenzie fiscali e doganali, e molti altri enti ancora. Tutto ciò a condizione che a tali enti e organismi siano attribuiti "autorità pubblica e i poteri pubblici" in rapporto a reati o minacce alla sicurezza pubblica che possano comportare attività di natura penale ricadenti nel rispettivo mandato operativo.

Si è già osservato, inoltre, che il trattamento di dati personali svolto dai soggetti di cui sopra in rapporto ad attività che esulano dall'ambito penale è disciplinato dal RGPD e non dalla direttiva, e lo stesso vale con riguardo al trattamento svolto da tali autorità in rapporto alle minacce alla sicurezza pubblica che non comportino reati – quali eventi atmosferici, inondazioni, epidemie, o la gestione di eventi sportivi per gli aspetti non riferiti alla possibile commissione di atti di natura penale.

iii. Trattamenti disciplinati

Per quanto riguarda gli strumenti utilizzati ai fini del trattamento, e conformemente con gli altri atti giuridici dell'Ue in materia di protezione dei dati, la direttiva polizia e giustizia si applica al

> trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

In altri termini, la direttiva si applica a tutti i trattamenti automatizzati di dati personali e al trattamento di ogni dato personale che sia contenuto in un archivio non automatizzato, purché esso ricada nell'ambito soggettivo e oggettivo di applicazione della direttiva stessa.

È importante osservare che, diversamente dalla Decisione quadro del 2008 sopra menzionata (v. paragrafo 1.3.6), la direttiva si applica non solo ai dati personali scambiati fra Stati membri, ma anche ai trattamenti di dati personali svolti a livello nazionale per finalità di polizia e giustizia. Come evidenziato dalla Commissione, la direttiva dovrebbe dunque "facilitare la cooperazione fra le autorità di polizia e giudiziarie in materia penale a livello dell'Ue".[172]

Libera circolazione dei dati fra autorità competenti nei singoli Stati membri

Benché la direttiva non pregiudichi "la facoltà degli Stati membri di prevedere garanzie più elevate di quelle in essa stabilite" (art. 1, paragrafo 3), lo Stato membro che ritenga di introdurre tali garanzie più elevate non può invocarle al fine di "limitare o vietare" la libera circolazione di dati personali fra gli Stati membri – ossia, ciò che costituisce l'obiettivo ultimo della direttiva stessa (art. 1, paragrafo 2, lettera b)). Peraltro, se uno Stato membro prevede attraverso la legislazione nazionale "condizioni specifiche" per

[172] Commissione europea, Scheda informativa - How will the data protection reform help fight international crime?, 30 aprile 2018, disponibile qui: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en.

determinati trattamenti (per esempio, la profilazione), o per il trattamento di determinate categorie di dati (per esempio, i dati biometrici), tale Stato membro non solo può, ma in effetti deve anche

"disp[orre] che l'autorità competente che trasmette i dati informi il destinatario di tali dati personali di tali condizioni e dell'obbligo di rispettarle". (Art. 9, paragrafo 3).

Tuttavia, gli Stati membri non possono, alla luce della disposizione suddetta, imporre ai destinatari di altri Stati membri che si occupino di questioni giudiziarie o di polizia condizioni diverse da quelle che essi prevedono per "trasmissioni" di dati "analoghe" verso destinatari nazionali della stessa tipologia (Articolo 9, paragrafo 4).

(Per quanto concerne i trasferimenti di dati personali verso Paesi terzi, si veda il relativo paragrafo, *infra*).

Contenuto delle disposizioni

Molte disposizioni della direttiva polizia e giustizia sono simili a quelle del RGPD, ma con alcuni distinguo che riflettono il particolare contesto delle attività di contrasto e di prevenzione delle minacce penali alla sicurezza pubblica.

Le **definizioni** dei concetti fondamentali di cui all'Art. 3 ("dato personale", "trattamento", "limitazione del trattamento", "profilazione", "pseudonimizzazione", "archivio", "titolare", "responsabile", "destinatario", "violazione di dati personali", "dati genetici", "dati biometrici", "dati relativi alla salute") sono identiche a quelle contenute nel RGPD.[173]

Anche i **principi fondamentali**, fissati all'Articolo 4, sono simili. In particolare, il principio di "liceità", assente nella Decisione-quadro del 2008, adesso è citato espressamente all'Articolo 4, lettera a), e ulteriormente sviluppato nelle disposizioni di cui all'Art. 8, paragrafo 1; mentre il principio di "trasparenza" (direttamente connesso al principio di liceità e correttezza nel RGPD) trova parziale rispecchiamento nel paragrafo 2 dell'Art. 8 ("*Il diritto dello Stato membro che disciplina il trattamento nell'ambito di applicazione della presente direttiva specifica quanto meno gli obiettivi del trattamento, i dati personali da trattare e le finalità del trattamento*") e nelle disposizioni sulle informazioni da fornire agli interessati e sull'accesso da parte di questi ultimi ai dati che li riguardano (anche se nel particolare contesto della direttiva tali diritti sono soggetti a maggiori limitazioni).

Il **principio di finalità è soggetto a limitazioni**, nel senso che i dati personali raccolti da qualsivoglia delle autorità competenti di cui sopra per finalità di applicazione della legge o di sicurezza pubblica possono essere utilizzati per altri scopi, a condizione che tale utilizzo sia "autorizzato dal diritto dell'Unione o dello Stato membro" (Art. 9, paragrafo 1, primo periodo), e salvo quanto previsto dal secondo periodo di tale paragrafo, ossia che

> Qualora i dati personali siano trattati per tali finalità diverse, si applica il regolamento (UE) 2016/679, a meno che il trattamento non sia effettuato nell'ambito di un'attività

[173] È singolare che, pur contenendo definizioni sostanzialmente identiche a quelle del GDPR, la direttiva non preveda una definizione di "terzi", mentre nella definizione di "destinatario" si fa espresso riferimento a soggetti terzi.

che non rientra nell'ambito di applicazione del diritto dell'Unione.[174]

Ne consegue che i dati provenienti da attività di polizia o giudiziarie che siano riutilizzabili sulla base di quanto "autorizzato" dalla legislazione nazionale devono comunque limitarsi a quelli "pertinenti" e "necessari" per lo scopo "legittimo" perseguito dalla legislazione stessa. **In linea di principio, questo è un ambito ove il RPD è chiamato a svolgere un ruolo essenziale, sia nei confronti degli enti che comunicano i dati sia nei confronti degli enti destinatari di tali dati**. Tuttavia, può avvenire che la norma si limiti a prevedere che, a determinate condizioni (per esempio, con l'autorizzazione di un dirigente), alcuni dati di questo tipo devono essere forniti ad agenzie non operanti nei settori giudiziari e di polizia.[175]

La direttiva impone agli Stati membri di prevedere **termini per la conservazione dei dati** trattati in base alle sue disposizioni (Art. 5); e di operare una **distinzione** fra i dati personali appartenenti a **categorie distinte di interessati** (persone sospettate di reati, condannati, vittime, testimoni, ecc.) (Art. 6). Essa prevede, inoltre, che "*Gli Stati membri dispongono che i dati personali fondati su fatti siano differenziati, nella misura del possibile, da quelli fondati su valutazioni personali*."

Analogamente al RGPD, la direttiva impone ai titolari l'adozione di misure di **sicurezza** in linea con lo "**stato dell'arte**", tenendo conto del contesto, degli scopi, ecc. del trattamento (Art. 29, paragrafo 1); i titolari devono condurre una **valutazione del rischio** al riguardo, per stabilire quale sia il livello adeguato di sicurezza (Art. 29, paragrafo 2). Inoltre, e sempre in analogia con il RGPD, la direttiva impone l'adozione di misure fisiche e tecniche di sicurezza e la previsione di **obblighi di riservatezza** in capo al personale dipendente (Art. 23).

Sussiste poi l'obbligo, come prevede anche il RGPD, di notificare all'autorità di controllo le **violazioni di dati personali**, entro 72 h (o di giustificare la ritardata notifica, eventualmente) (Art. 30); gli interessati devono esserne informati "*senza ingiustificato ritardo*" "*quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche*" (Art. 31).

Le norme della direttiva concernenti il trattamento di **dati sensibili** (ossia, dei dati che "rivelano l'origine razziale o etnica, le opinioni politiche, le credenze filosofiche o religiose, o l'appartenenza sindacale", dei dati genetici, dei dati biometrici (se utilizzati allo scopo di identificare univocamente una persona fisica), "dei dati relativi alla salute" dei dati "relativi alla vita sessuale o all'orientamento sessuale di una persona fisica") sono strutturate in modo parzialmente diverso rispetto al RGPD (Art. 9)[176], poiché la

---

[174] Si veda anche l'art. 9, paragrafo 2. Sul punto, vedi anche il paragrafo 1.4.6, *infra*.

[175] Si pensi alle controversie sulla proposta presentata alcuni anni fa nel RU di condividere le informazioni sui minori fra vari enti (assistenza sociale, autorità di polizia, scuole). Vedi: Ross Anderson *et al.*, Children's Databases – Safety and Privacy: A Report for the Information Commissioner, prepared by the UK Foundation for Information Policy research (FIPR), 2006, comprendente anche sintesi (redatte da Douwe Korff) non solo nella pertinente normativa del RU ma anche (in appendice) una panoramica della legislazione in altri paesi europei, in particolare in Germania e Francia. Disponibile qui: https://www.cl.cam.ac.uk/~rja14/Papers/kids.pdf

[176] Come è lecito aspettarsi, la direttiva non contiene una disposizione analoga all'Art. 10 del RGPD, primo periodo, in base alla quale il trattamento di dati personali relativi a condanne penali e reati deve "*avvenire sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o dello Stato membro*

direttiva consente il trattamento dei dati in questione:

> "**solo** se **strettamente necessario**, soggetto a **garanzie adeguate** per i diritti e le libertà dell'interessato e soltanto:
>
> a) se **autorizzato** dal **diritto** dell'Unione o dello Stato membro;
>
> b) per salvaguardare un **interesse vitale** dell'interessato o di un'altra persona fisica; o
>
> c) se il suddetto trattamento riguarda dati **resi manifestamente pubblici dall'interessato**."

(Art. 10 DPDPG).

Le due ultime condizioni corrispondono a deroghe al divieto di trattare tali dati come previste nel RGPD (Art. 9, paragrafo 2, lettere c) ed e)). [177]

Qualora uno Stato membro faccia riferimento all'altra condizione, ossia il fatto che il trattamento è **autorizzato dal diritto**, deve poter dimostrare che si tratta di un trattamento "***strettamente necessario***" e che eventuali limiti ai diritti degli interessati sono "***soggetti a garanzie adeguate***". Inoltre, e diversamente da quanto avveniva con la decisione quadro del 2008, i singoli possono invocare direttamente le norme della direttiva per ottenere il rispetto dei diritti loro riconosciuti dinanzi alla Corte di giustizia dell'Ue, l'organo in ultima analisi deputato a stabilire se una normativa nazionale in questo ambito soddisfi il parametro della "stretta necessità" e contenga "garanzie adeguate"; per altro verso, la Commissione adesso ha il potere di agire nei confronti di uno Stato membro qualora ritenga che il diritto nazionale di tale Stato autorizzi il trattamento di dati sensibili per scopi di polizia e giustizia secondo modalità difformi dai parametri suddetti.

Come il RGPD, la direttiva disciplina i **processi decisionali automatizzati compresa la profilazione**, ma con alcune differenze. In particolare, essa prevede che questi trattamenti debbano essere "*autorizzati dal diritto dell'Unione o dello Stato membro*" e soggetti a "garanzie adeguate" che devono comprendere "*almeno il diritto di ottenere l'intervento umano da parte del titolare*". Tuttavia, a differenza del RGPD, la direttiva non prevede che a tale "intervento umano" si associ la possibilità per l'interessato di "esprimere il proprio punto di vista e… opporsi alla decisione [automatizzata/fondata sulla profilazione]".

In particolare, la direttiva stabilisce quanto segue:

---

che preveda garanzie appropriate per i diritti e le libertà degli interessati". La direttiva stessa e le relative leggi nazionali in materia contengono norme al riguardo. Analogamente, non trova rispecchiamento nella direttiva la disposizione di cui all'Art. 10, ultimo periodo, del RGPD, per cui "*Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica*".

[177] Con la differenza che la deroga relativa all'interesse vitale della persona interessata o di un terzo di cui all'Art. 9(2), lettera c), RGPD si applica solo se "l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso" – requisito quest'ultimo non contemplato nella Direttiva.

> **La profilazione che porta alla discriminazione di persone fisiche sulla base di categorie particolari di dati personali di cui all'articolo 10 è vietata**, conformemente al diritto dell'Unione.

Rispetto alla tematica della "autorizzazione" ai sensi del diritto nazionale o dell'Ue, è importante anche tenere presente l'obbligo di consultare la competente autorità nazionale di controllo nell'elaborazione di proposte legislative su tali materie (Art. 28, paragrafo 2).

I RPD che operano nelle singole autorità devono valutare attentamente in che modo dare reale ed effettiva applicazione, nei vari contesti, a questi importanti e innovativi requisiti fissati dalla DPDPG – ossia, l'intervento umano e l'obbligo di non discriminazione.

Alla luce dell'ambito di applicazione che le è proprio, la DPDPG consente ampie **limitazioni dei diritti degli interessati** di essere informati del trattamento, di accedere ai propri dati, e di ottenere la rettifica o la cancellazione dei dati che non soddisfano i parametri di qualità in essa previsti o sono comunque trattati in violazione delle norme in essa contenute; tuttavia, tali limitazioni non possono travalicare quanto è "necessario" e "proporzionato" in una società democratica (v. Artt. 12-16 DPDPG, in particolare Art. 15). La direttiva consente anche **l'esercizio indiretto** di tali diritti, attraverso la competente autorità di controllo (Art. 17). Ove i dati personali "figurino in una decisione giudiziaria, in un casellario o in un fascicolo giudiziario oggetto di trattamento nel corso di un'indagine e di un procedimento penale", i diritti in parola possono essere anche disciplinati dal diritto interno applicabile (Art. 18). Tipicamente è la **legislazione che regolamenta le attività di polizia ovvero un codice di procedura penale** a disciplinare l'accesso a determinate parti di un fascicolo procedimentale, in determinate fasi del procedimento, da parte di persone sospettate, accusate, imputate o condannate a seguito della commissione di un reato; in genere l'accesso è consentito in misura limitata nelle fasi iniziali del procedimento ed è invece soggetto a minori restrizioni nelle fasi successive, soprattutto dopo la formalizzazione delle accuse. Tutti questi meccanismi sono quindi compatibili con il regime giuridico della DPDPG.

Requisiti formali e sostanziali

La DPDPG introduce requisiti formali e sostanziali che, anche sotto numerosi altri riguardi, si avvicinano a quelli fissati nel RGPD.

Particolare importanza riveste il "**principio di responsabilizzazione**" introdotto dalla DPDPG (Art. 19, paragrafo 4), come già dal RGPD, in base al quale "tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche", il titolare soggetto alla direttiva stessa deve

> mettere in atto misure tecniche e organizzative adeguate **per garantire, ed essere in grado di dimostrare**, che il trattamento è effettuato ai sensi della presente direttiva. (Art. 19, paragrafo 1)

Il testo dell'articolo in questione precisa poi che "tali misure sono riesaminate e aggiornate qualora necessario" e che "Se ciò è proporzionato" rispetto alle attività di

trattamento, esse includono "l'attuazione di politiche adeguate in materia di protezione dei dati" da parte del titolare del trattamento (Art. 19, paragrafo 1, ultimo periodo, e paragrafo 2).

Come il RGPD, la direttiva prevede obblighi di tenuta di un registro dei trattamenti e di registrazione dei trattamenti (Artt. 24 e 25), in quanto strumenti fondamentali per assicurare la verificabilità della liceità dei trattamenti stessi – obiettivo di particolare complessità nelle materie soggette all'applicazione della DPDPG.

La direttiva prevede gli stessi requisiti del RGPD per quanto concerne eventuali "contitolari" del trattamento (Art. 21, pragrafo 2) e il ricorso a responsabili del trattamento (Art. 22).

Essa prevede l'obbligo di condurre una valutazione d'impatto della protezione dei dati (DPIA, Art. 27) in circostanze analoghe a quelle indicate nel RGPD, ossia

> Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche (Art. 27)

L'autorità di controllo competente, che può essere l'autorità nazionale di protezione dati, ma potrebbe anche essere una diversa autorità purché siano garantiti i requisiti di indipendenza, ecc. – v. *infra* - , **deve essere consultata** quando una valutazione di impatto "*indica che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio*" oppure, a prescindere dall'adozione di tali eventuali misure, "*il tipo di trattamento, in particolare se utilizza tecnologie, procedure o meccanismi nuovi, presenta un rischio elevato per i diritti e le libertà degli interessati*" (Art. 28, paragrafo 1, lettere a) e b)).

Quale strumento atto a contribuire all'efficace applicazione della norma, con particolare riguardo al principio di responsabilizzazione, la direttiva prevede la designazione di un **responsabile della protezione dei dati (RPD/DPO**, Data Protection Officer) da parte di ogni titolare (Art. 32), ne illustra le caratteristiche soggettive (Art. 33) e ne elenca i compiti (Art. 34). Anche in questo caso il modello è il RGPD, il quale prevede la designazione di un RPD da parte di tutti i soggetti pubblici cui esso è applicabile[178]. Tuttavia, la DPDPG non richiede espressamente che il RPD sia in grado di agire in modo indipendente.[179]

I RPD operanti presso le autorità di polizia o giudiziarie o presso ogni altra agenzia o ente che ricada nel campo di applicazione della DPDPG avranno un ruolo essenziale

[178] V. Parte II, paragrafo 2.4.2., *infra*.

[179] Si veda l'art. 38, paragrafo 3, del RGPD, in base al quale "*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*."

nel garantire l'osservanza del principio di responsabilizzazione e la revisione permanente delle misure adottate a tale scopo, nonché nella redazione degli "accordi" con eventuali contitolari di trattamento e dei contratti da stipulare con i responsabili di trattamento, nelle attività di consultazione della competente autorità di controllo, e nella conduzione di valutazioni di impatto ai sensi della DPDPG.[180]

Trasferimenti internazionali di dati verso autorità competenti in Paesi terzi

Alla luce della delicatezza dei contesti e dei dati personali coinvolti, il Capo V della DPDPG prevede una serie di condizioni il cui soddisfacimento è necessario ai fini del trasferimento di dati personali verso un Paese extra-Ue ("Paese terzo") o verso un'organizzazione internazionale, sulla falsariga di quelle indicate nel RGPD, con l'aggiunta di norme ulteriori che disciplinano i trasferimenti verso un Paese terzo o un'organizzazione internazionale da parte di uno Stato membro dell'Ue di dati personali ricevuti da un altro Stato membro, nonché sui trasferimenti ulteriori da parte del Paese terzo di destinazione dei dati in oggetto verso un altro Paese terzo o un'organizzazione internazionale. Sono previste anche eccezioni più specifiche in presenza di specifiche situazioni, come vedremo nel prosieguo.

Si osservi però che, con particolare riguardo ai trasferimenti internazionali di dati, la direttiva prevede una tempistica più dilatata ai fini della piena applicazione delle norme esaminate in appresso, per motivi specifici che sono meglio illustrati nel paragrafo dal titolo "Recepimento ritardato" al termine di questa sezione dedicata alla DPDPG.

Requisiti preliminari di carattere generale ai fini dei trasferimenti in oggetto:

L'Art. 35 della DPDPG fissa **tre requisiti preliminari** ai fini di ogni trasferimento verso un Paese terzo (si osservi però che *in alcune circostanze due di tali requisiti preliminari possono essere disapplicati*, v. *infra*):

- il trasferimento deve essere "**necessario**" per le finalità di cui all'Art. 1(1) della direttiva, ossia per la prevenzione, le indagini, l'accertamento o il perseguimento di reati o l'esecuzione di condanne penali, ovvero per la salvaguardia contro o la prevenzione di minacce (penali/giuridiche) alla sicurezza pubblica;
- il trasferimento deve avvenire verso **un'autorità nel Paese terzo o un'organizzazione internazionale che sia competente ai fini di cui sopra** (e l'Interpol rientra espressamente in questo novero ai sensi del Considerando n. 25). [181] Così come le "autorità competenti" nell'Ue non si limitano alle forze

[180] Si veda l'analisi dettagliata dei compiti del RPD ai sensi del RGPD di cui alla Parte III del presente Manuale.

[181] Al riguardo, si osservi che l'Interpol non costituisce una "organizzazione internazionale" nel senso normalmente attribuito a tale espressione in base al diritto internazionale pubblico, ossia un'organizzazione che si fonda su un trattato o è stata comunque istituita ai sensi del diritto internazionale: si veda l'Art. 2 del progetto di articolato sulla responsabilità delle organizzazioni internazionali elaborato dalla International Law Commission. Viceversa, l'Interpol è stata istituita dalle autorità di polizia degli Stati partecipanti. Sul punto, si veda il quesito posto alla Commissione europea dal parlamentare europeo Charles Tannock il 15 ottobre 2013, (https://www.europarl.europa.eu/sides/getDoc.do?type=WQ&reference=E-2013-011707&language=EN) e la

dell'ordine e alle autorità giudiziarie, anche le autorità dei Paesi terzi alle quali i dati possono essere trasferiti non devono necessariamente limitarsi a quelle direttamente operanti nel settore dell'applicazione della legge purché siano competenti (anche) in rapporto a materie di natura penale di loro pertinenza.
Si osservi che *tale requisito preliminare non trova applicazione in determinate circostanze* e a determinate condizioni: si veda *infra* il paragrafo "Trasferimento ad altre autorità".

- "*qualora i dati personali siano trasmessi o resi disponibili da un altro Stato membro, tale Stato membro ha fornito la propria* ***autorizzazione preliminare*** *al trasferimento conformemente al proprio diritto nazionale*" (salve alcune eccezioni, v. *infra*.)
(Art. 35(1), lettere a)-c))

Tale ultima condizione riguarda il trasferimento da uno Stato membro verso un Paese terzo o un'organizzazione internazionale di dati personali che tale Stato membro aveva ricevuto da un altro Stato membro: ossia, il trasferimento ulteriore dei dati in questione necessita della "autorizzazione preliminare" dello Stato membro che aveva fornito inizialmente i dati.
Si osservi che l'autorizzazione preliminare in questione non è richiesta se:

> il trasferimento di dati personali è **necessario per prevenire una minaccia grave e immediata alla sicurezza pubblica di uno Stato membro o di un paese terzo o agli interessi vitali di uno Stato membro** e l'autorizzazione preliminare non può essere ottenuta tempestivamente.

In tal caso, "L'autorità competente a rilasciare l'autorizzazione preliminare [ossia, l'autorità cui si sarebbe dovuto chiedere l'autorizzazione preliminare se non vi fosse stata tale minaccia immediata] è informata senza indugio." (Art. 35, paragrafo 2).

Una volta soddisfatti tali requisiti preliminari, in quanto applicabili, il trasferimento di

---

risposta fornita dalla Commissione (https://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2013-011707&language=EN). Tuttavia, l'Interpol continua spesso a essere considerata alla stregua di un'organizzazione internazionale, in qualche misura anche dalla stessa Ue, che ha adottato una Posizione comune del Consiglio sullo scambio di dati contenuti nei passaporti con l'Interpol e gli Stati partecipanti all'Interpol, salve le garanzie in materia di protezione dei dati: Posizione comune del Consiglio 2005/69/GAI del 24 gennaio 2005 sullo scambio di determinati dati con l'Interpol, GU L 29 gennaio 2005, p. 61, disponibile qui: https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A32005E0069 (per gli aspetti di protezione dei dati, v. Art. 3). Si veda anche la Decisione del Consiglio 2007/533/GAI del 12 giugno 2007 sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II); GU L 205, 7 agosto 2007, p. 63, in cui si vieta il trasferimento o la messa a disposizione di dati provenienti dal SIS-II a paesi terzi e organizzazioni internazionali (Art. 54) fatta eccezione per gli scambi di dati con Interpol relativi a passaporti rubati, altrimenti sottratti, smarriti o falsificati (Art. 55) (https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32007D0533&from=EN). Il considerando 25 della DPDPG sembra indicare che tale strumento consenta una più ampia condivisione di dati con e attraverso l'Interpol, a condizione che siano soddisfatte le condizioni generali che disciplinano i trasferimenti di dati verso organizzazioni internazionali e paesi terzi di cui alla direttiva stessa.

dati personali verso un Paese terzo o un'organizzazione internazionale è consentito se ricorre **almeno una delle seguenti condizioni**:

- la Commissione ha adottato una **decisione di adeguatezza** nei confronti del Paese terzo o dell'organizzazione internazionale di destinazione dei dati (secondo quanto previsto dal successivo Art. 36).

  Si osservi però che la Commissione europea non ha, a oggi, adottato alcuna decisione di adeguatezza ai sensi di tale disposizione, che quindi non trova alcuna applicazione al momento;

  oppure:

- esistono "**garanzie adeguate**" onde assicurare che, successivamente al trasferimento, i dati personali continueranno a essere trattati nel rispetto di "adeguate" garanzie in termini di protezione dei dati.
  Sul punto fa ulteriore chiarezza l'Art. 37, prevedendo che le garanzie in questione siano fissate in uno **strumento giuridicamente vincolante** (un trattato, un accordo amministrativo di carattere vincolante – Art. 37(1), lettera a)) ovvero che "il titolare del trattamento ha **valutato** tutte le circostanze relative al trasferimento dei dati personali e ritiene che sussistano garanzie adeguate per la protezione dei dati personali" (Art. 37(1), lettera b)). Tuttavia, in quest'ultimo caso è necessario informare l'autorità di controllo delle "categorie di trasferimenti" effettuati sul fondamento della disposizione suddetta. Inoltre, ciascuno di tali trasferimenti deve essere "documentato e, su richiesta, la documentazione deve essere messa a disposizione dell'autorità di controllo con l'indicazione della data e dell'ora del trasferimento, delle informazioni sull'autorità competente ricevente, della motivazione del trasferimento e dei dati personali trasferiti." (Art. 37, paragrafo 3).
  Si osservi che gli "strumenti giuridicamente vincolanti" di cui sopra comprendono "accordi internazionali relativi al trasferimento di dati personali verso paesi terzi od organizzazioni internazionali conclusi dagli Stati membri anteriormente al 6 maggio 2016", come stabilisce l'art. 61 DPDPG. Sempre in base a tale articolo, gli accordi in questione "restano in vigore fino alla loro modifica, sostituzione o revoca" a condizione che essi siano "conformi al diritto dell'Unione applicabile prima di tale data". La DPDPG non fissa un termine ultimo per la modifica, sostituzione o revoca degli accordi eventualmente non conformi alle norme in essa contenute, né impone agli Stati membri di provvedere alla revisione di tali accordi ai fini suddetti. Sul punto, vedi *infra* il paragrafo dal titolo "Recepimento ritardato";

  oppure
- (in assenza di una decisione di adeguatezza ai sensi dell'Art. 36 e di garanzie adeguate ai sensi dell'Art. 37) se trova applicazione una delle **deroghe in specifiche situazioni**. L'Art. 38 consente il ricorso a tali deroghe se il trasferimento è "**necessario**" in **cinque diverse situazioni**, due delle quali richiedono un "bilanciamento" degli interessi in gioco. Le situazioni e condizioni specifiche sono le seguenti (enumerate in ordine diverso da quello utilizzato nell'articolo):
  - Il trasferimento di dati personali verso un paese terzo in assenza di una decisione di adeguatezza e di garanzie adeguate è consentito se è "necessario" per uno degli scopi di cui all'Art. 1, paragrafo 1, ossia ai fini della prevenzione, delle indagini, dell'accertamento o del perseguimento di reati o dell'esecuzione di condanne penali, o per la salvaguardia contro

o la prevenzione di minacce (penali/giuridiche) alla sicurezza pubblica (Art. 38(1), lettera d)), salvo che

- L'autorità competente che opera il trasferimento determin[i] che i diritti e le libertà fondamentali dell'interessato prevalgono sull'interesse pubblico al trasferimento (Art. 38, paragrafo 2)

- Il trasferimento di dati personali verso un paese terzo in assenza di una decisione di adeguatezza e di garanzie adeguate è consentito se è "necessario" per accertare, esercitare o difendere un diritto in sede giudiziaria con riguardo a una delle finalità di cui sopra (Art. 38(1), lettera e)), di nuovo salvo che
  - L'autorità competente che opera il trasferimento determin[i] che i diritti e le libertà fondamentali dell'interessato prevalgono sull'interesse pubblico al trasferimento (Art. 38, paragrafo 2)

Si osservi che le due situazioni sopra descritte riguardano casi che sollevano difficili problematiche in tema di diritti umani: da un lato, il trasferimento risulta "necessario" per un interesse pubblico importante; d'altro canto esso incide sui diritti e le libertà fondamentali dell'interessato, magari in termini devastanti – per esempio, se informazioni su una persona sospettata, testimone o vittima di un reato sono trasferite alle autorità di uno stato responsabile di gravi violazioni dei diritti umani, e non vi sono "garanzie adeguate" anche per quanto riguarda il trattamento ulteriore dei dati personali in oggetto. **È chiaro che si dovrà consultare il RPD dell'autorità competente prima di procedere a trasferimenti di questo tipo, e il RPD non avrà compito facile nel fornire la consulenza richiesta**.

- Il trasferimento di dati personali verso un paese terzo in assenza di una decisione di adeguatezza e di garanzie adeguate è consentito se è **"necessario" per la prevenzione di una minaccia grave e immediata alla sicurezza pubblica di uno Stato membro o di un paese terzo** (Art. 38(1), lettera c)) – apparentemente in questo caso si prescinde da valutazioni dell'impatto sui diritti e le libertà fondamentali dell'interessato (a meno che il requisito della "necessità" del trasferimento sia da intendersi in tal senso?).
- Il trasferimento di dati personali verso un paese terzo in assenza di una decisione di adeguatezza e di garanzie adeguate è consentito se è "**necessario" per la tutela degli interessi vitali dell'interessato o di un terzo** (Art. 38(1), lettera a)).
- Il trasferimento di dati personali verso un paese terzo in assenza di una decisione di adeguatezza e di garanzie adeguate è consentito se è "**necessario" per la salvaguardia di legittimi interessi dell'interessato**, qualora lo preveda il diritto dello Stato membro che trasferisce i dati personali (Art. 38(1), lettera b)).

I dati trasferiti sulla base di una delle cinque deroghe sopra descritte devono essere "**strettamente necessari**" (Considerando 72) e **documentati**, e

su richiesta, la documentazione deve essere messa a disposizione dell'autorità di controllo con l'indicazione della data e dell'ora del trasferimento, delle informazioni sull'autorità competente ricevente, della motivazione del trasferimento e dei dati personali trasferiti (Art. 38, paragrafo

3)

Questi obblighi di documentazione e di messa a disposizione dell'autorità di controllo intendono consentire all'autorità stessa di "monitorare (*retrospettivamente*) la liceità del trasferimento" (Considerando 72). Tale ultimo considerando aggiunge quanto segue:

> Tali deroghe dovrebbero essere **interpretate in modo restrittivo** e **non dovrebbero consentire trasferimenti frequenti, ingenti e strutturali** di dati personali o trasferimenti su larga scala di dati, ma andrebbero invece limitate ai dati strettamente necessari.

Ancora una volta, rileviamo le importanti responsabilità che ricadono su ogni RPD operante presso una delle autorità competenti con riguardo a tali obblighi di documentazione, nonché a tutte le interazioni con l'autorità di controllo nelle materie pertinenti.[182]

Trasferimenti ad altre autorità in paesi terzi

Abbiamo già osservato che, in linea di massima, tutte le tre tipologie di trasferimenti sopra descritte possono aver luogo con riguardo ad autorità che, nei singoli paesi terzi, sono investite di competenze rispetto alle finalità di cui all'Art. 1(1) della DPDPG – ossia, "prevenzione, indagine, accertamento e perseguimento di reati, comprese la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica" (Art. 35(1), lettera b)) – anche se i destinatari dei dati non devono essere necessariamente soggetti appartenenti alle forze di polizia o al mondo giudiziario, potendo comprendere anche altre autorità pubbliche i cui compiti e poteri siano connessi in parte al settore penale o alla sicurezza pubblica.

Tuttavia, l'art. 39 della DPDPG prevede alcune **eccezioni** a tale regola e disciplina i "Trasferimenti di dati personali verso destinatari stabiliti in paesi terzi" – intendendo con ciò destinatari diversi dalle autorità competenti, nei singoli paesi terzi, per le materie di cui all'Art. 1, paragrafo 1, della direttiva stessa.

Le motivazioni alla base di tali eccezioni sono illustrate nel Considerando 73:

> Le autorità competenti degli Stati membri applicano accordi internazionali bilaterali o multilaterali vigenti, conclusi con paesi terzi nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia, ai fini dello scambio di informazioni pertinenti affinché possano eseguire i compiti assegnati loro dalla legge. In linea di principio, ciò avviene tramite o almeno con la cooperazione delle autorità competenti nei paesi terzi interessati ai fini della presente direttiva, talvolta persino in mancanza di un accordo internazionale bilaterale o multilaterale.
>
> **Tuttavia, in singoli casi specifici, le normali procedure che richiedono di contattare tale autorità nel paese terzo possono risultare inefficaci o inadatte, in particolare in quanto il trasferimento non potrebbe essere effettuato tempestivamente, o in quanto detta autorità nel paese terzo non rispetta lo stato di diritto o le norme e gli standard internazionali in materia di diritti dell'uomo, cosicché le autorità competenti degli Stati membri potrebbero decidere di trasferire i dati personali direttamente ai destinatari stabiliti in detti paesi terzi**.

[182] Si veda la Parte III del Manuale, Compiti del RPD, Compiti 1-5 e 12.

Ciò potrebbe verificarsi qualora vi sia urgente necessità di trasferire dati personali per salvare la vita di una persona che rischia di essere vittima di un reato o al fine di evitare l'imminente commissione di un reato, anche terroristico.

Anche se detto trasferimento tra autorità competenti e destinatari stabiliti in paesi terzi dovrebbe prodursi unicamente in singoli casi specifici, la presente direttiva dovrebbe stabilire le condizioni per regolamentare tali casi.

Dette disposizioni non dovrebbero essere considerate alla stregua di deroghe ad accordi internazionali bilaterali o multilaterali vigenti nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia. Tali norme dovrebbero applicarsi in aggiunta alle altre disposizioni della presente direttiva, in particolare quelle sulla liceità del trattamento e quelle del capo V.

Il testo dell'Art. 39, paragrafo 1, può essere parafrasato come segue:[183]

> Il diritto dell'Ue o di uno Stato membro può disporre che le autorità incaricate dell'applicazione della legge, in casi singoli e specifici, trasferiscano dati personali direttamente a destinatari stabiliti in Paesi terzi che non hanno competenze in materie penali o connesse alla sicurezza pubblica, purché siano rispettate le altre disposizioni della presente direttiva e siano soddisfatte tutte le seguenti condizioni:…

La direttiva tace sulla natura specifica delle "altre autorità" in parola. Visto che l'art. 39 trova applicazione in circostanze particolarmente delicate in termini di tutela dei diritti umani (si veda il paragrafo sopra evidenziato all'interno del considerando 73), si deve ritenere che ci si riferisca a destinatari nel paese terzo che godono di **particolare fiducia** da parte dell'autorità nel singolo Stato membro dell'Ue che trasmette i dati. In particolare, quest'ultima autorità deve aver modo di ritenere che il destinatario, diverso da una delle autorità competenti come sopra definite, non trasmetterà le informazioni a una di tali autorità del Paese terzo che "non riseptta lo stato di diritto o le norme e gli standard internazionali in materia di diritti dell'uomo". La necessaria valutazione caso per caso rivestirà sempre particolare delicatezza, e dovrà essere quanto meno **documentata con la massima scrupolosità** (comprese le ragioni per cui si è giunti alla conclusione che i dati potessero essere trasmessi a un siffatto destinatario affidabile senza timore che finissero successivamente in mani meno fidate nello specifico paese terzo.)

Per quanto riguarda i trasferimenti non fondati su accordi internazionali (v. *infra*), l'art. 39, paragrafo 1, prevede cinque condizioni cumulative. I dati possono essere trasferiti a un destinatario in un paese terzo diverso dalle suddette "autorità competenti" se:

a. Il trasferimento è strettamente necessario all'assolvimento di un compito dell'autorità competente che trasferisce i dati [nel singolo Stato membro Ue] conformemente al diritto dell'Unione o dello Stato membro e per le finalità di cui all'art. 1, paragrafo 1 [ossia, in rapporto a materie penali o di sicurezza pubblica nell'Ue o nel singolo Stato membro];
b. L'autorità competente che trasferisce i dati determina che non sussistono diritti

[183] Il testo dell'Articolo 39, paragrafo 1, è il seguente:
"*In deroga all'articolo 35, paragrafo 1, lettera b), e fatti salvi eventuali accordi internazionali di cui al paragrafo 2 del presente articolo, il diritto dell'Unione o dello Stato membro può disporre che le autorità competenti di cui all'articolo 3, punto 7), lettera a), possano, in casi singoli e specifici, trasferire dati personali direttamente a destinatari stabiliti in paesi terzi soltanto se le altre disposizioni della presente direttiva sono rispettate e se sono soddisfatte tutte le seguenti condizioni*:…"

e libertà fondamentali dell'interessato prevalenti rispetto all'interesse pubblico che rende necessario il trasferimento nel caso specifico.
Si osservi che tale determinazione non si limita agli interessi di cui l'interessato è portatore in termini di protezione dei dati, dovendosi in realtà stabilire, più in generale, se il singolo paese terzo e le singole agenzie o i singoli organismi in tale paese "*rispettano lo stato di diritto o le norme e gli standard internazionali in materia di diritti dell'uomo*". Inoltre, si tratta di una determinazione da effettuare **caso per caso**.

c. L'autorità competente che trasferisce i dati ritiene che **il trasferimento a un'autorità competente per le finalità di cui all'Art. 1, paragrafo 1** [materie penali e di sicurezza pubblica] nel paese terzo **sia inefficace o inadatto**, in paticolare perché non può essere effettuato tempestivamente
oppure, si dovrebbe aggiungere, perché un tale trasferimento sarebbe "inadatto" per altri motivi: v. la nota aggiunta alla clausola successiva.

d. **L'autorità competente per le finalità di cui all'Art. 1, paragrafo 1, nel paese terzo ne è informata**, senza ingiustificato ritardo, a meno che ciò risulti **inefficace o inadatto**.
Si osservi che il riferimento alla circostanza per cui sarebbe "inadatta" la trasmissione dei dati a un'agenzia (di polizia e/o giudiziaria) che in condizioni normali sarebbe quella più pertinente e idonea può essere interpretato come un riferimento a situazioni in cui una tale agenzia "non rispetta lo stato di diritto o le norme e gli standard internazionali in materia di diritti dell'uomo". Il riferimento alla "inefficacia" di tale agenzia può lasciare intendere che essa operi altrimenti in modo inefficace, tardivo, incompetente o forse corrotto.

e. L'autorità competente che trasferisce i dati informa il destinatario della o delle finalità per cui i dati personali possono essere trattati dal destinatario stesso, a condizione che tale trattamento sia necessario.
Si osservi che ciò comporta l'obbligo per l'autorità ricevente nel paese terzo di fornire **garanzie** (forti e vincolanti) in merito al rispetto di tali prescrizioni, in particolare quanto all'uso delle informazioni fornite dall'autorità competente dello Stato membro Ue per lo scopo specifico e previsto e per nessun' altra finalità; e anche in tal caso, l'autorità ricevente dovrà impegnarsi a utilizzare le informazioni nella misura strettamente necessaria per gli scopi suddetti.

Oltre al rispetto di tutte le prescrizioni specifiche sopra ricordate, l'art. 39, paragrafo 1, sottolinea l'obbligo di osservare "tutte le altre disposizioni della presente direttiva" (v. anche l'ultimo periodo del considerando (73) sopra citato, dove si evidenzia come ciò comprenda "in particolare le disposizioni sulla liceità del trattamento e quelle del Capo V" – ossia, le altre disposizioni in materia di trasferimenti di dati).

Tuttavia, vengono fatti salvi in ogni caso "eventuali accordi internazionali" (Art. 39(1)), nel senso di

> qualsiasi accordo internazionale bilaterale o multilaterale in vigore tra gli Stati membri e paesi terzi nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia (Art. 39, paragrafo 2).

Tale disposizione va letta in combinato con l'Art. 61, concernente i rapporti fra la DPDPG e "accordi internazionali precedentemente conclusi nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia", in base al quale

> Restano in vigore, fino alla loro modifica, sostituzione o revoca, gli accordi internazionali

> relativi al trasferimento di dati personali verso paesi terzi o organizzazioni internazionali che sono stati conclusi dagli Stati membri anteriormente al 6 maggio 2016 e che sono conformi al diritto dell'Unione applicabile anteriormente a tale data

La direttiva non fissa un termine per la modifica, sostituzione o revoca di tali accordi, ove non conformi alle norme della direttiva stessa, né prevede un obbligo per gli Stati membri di rivedere tali accordi al fine di allinearli alle previsioni della direttiva[184]. Tuttavia, l'Art. 62 di quest'ultima in effetti stabilisce quanto segue:

> Entro il 6 maggio 2022 e, successivamente, ogni quattro anni, la Commissione trasmette al Parlamento europeo e al Consiglio una relazione di valutazione e sul riesame della presente direttiva. Tale relazione è pubblicata

Tale riesame deve comprendere "in particolare l'applicazione e il funzionamento del Capo V sul trasferimento di dati personali verso paesi terzi o organizzazioni internazionali" (Art. 62, paragrafo 2), con particolare riguardo alle decisioni di adeguatezza di cui all'Art. 36, paragrafo 3, e ai trasferimenti verso "altre autorità" di cui all'Art. 39. Inoltre, la Commissione può "chiedere informazioni agli Stati membri e alle autorità di controllo" in questo ambito (Art. 62, paragrafo 3) – compresi, si immagina, eventuali accordi internazionali precedentemente conclusi. Si può ipotizzare, inoltre, che sulla base di questo primo riesame la Commissione proponga eventuali emendamenti da apportare agli accordi in oggetto, o formuli almeno alcuni suggerimenti per garantirne l'allineamento con le norme della DPDPG – anche se non vi sono disposizioni specifiche al riguardo (diversamente da quanto vale per gli strumenti dell'Ue in questo settore).[185]

Secondo la Commissione, la DPDPG favorirà un "**potenziamento della cooperazione internazionale**"[186]:

> Sarà anche potenziata la cooperazione fra le autorità di polizia e giudiziarie penali dell'Ue e i paesi terzi, poiché saranno in vigore norme più chiare ai fini dei trasferimenti internazionali di dati concernenti reati. Queste nuove norme garantiranno che i trasferimenti avvengano con un livello adeguato di protezione dei dati.

Tuttavia, come osservato *infra* con riguardo al "Recepimento ritardato", passerà ancora del tempo prima dell'effettiva e piena applicazione delle nuove norme di cui sopra.

Vigilanza e attuazione delle norme

Il Capo VI della DPDPG prevede la creazione di autorità di controllo indipendenti negli Stati membri, con il compito di monitorare e garantire l'applicazione delle disposizioni di diritto interno adottate al fine di "trasporre" la direttiva stessa, e incaricate anche di altre funzioni a ciò connesse (v. Artt. 41-46 DPDPG). L'autorità di controllo in questione

[184] Né risultano analisi condotte prima dell'introduzione della DPDPG sulla conformità al diritto dell'Unione all'epoca vigente degli accordi internazionali conclusi precedentemente dagli Stati membri e che comportassero il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali.

[185] L'Art. 62, paragrafo 6, prevede che, entro il 6 maggio 2019, la Commissione sottoponga a riesame "gli altri atti giuridici adottati dall'Unione che disciplinano il trattamento da parte delle autorità competenti per le finalità di cui all'articolo 1, paragrafo 1, in particolare quelli di cui all'articolo 60, al fine di valutare la necessità di allinearli alla presente direttiva e formulare, ove opportuno, le proposte necessarie per modificarli in modo da garantire un approccio coerente alla protezione dei dati personali nell'ambito della presente direttiva". Si veda *infra* alla voce "Recepimento ritardato".

[186] Scheda informativa della Commissione europea – How will the data protection reform help fight international crime? (nota 172, *supra*).

può essere, ma non è detto che sia, l'autorità di controllo istituita ai sensi del RGPD (Art. 41, paragrafo 3). In alcuni Paesi esistono infatti specifiche autorità di controllo aventi il compito di vigilare sul trattamento di dati personali da parte delle autorità di polizia e giudiziarie; in altri Paesi è l'autorità di protezione dati generale a svolgere anche questo compito. Inoltre, in alcuni Paesi (soprattutto quelli a ordinamento federale) esistono più autorità di controllo, a livello nazionale (federale) e locale/regionale.

Analogamente alle autorità di controllo designate ai sensi del RGPD, le autorità di controllo competenti per le materie disciplinate dalla DPDPG devono godere di ampi poteri, compreso il diritto di chiedere (e ottenere) "accesso a tutti i dati personali oggetto di trattamento e a tutte le informazioni necessarie per l'adempimento dei rispettivi compiti", nonché del potere di rivolgere avvertimenti a un titolare o responsabile del trattamento, di ingiungere a tale titolare o responsabile di modificare operazioni di trattamento al fine di allinearle alla direttiva "se del caso, in una determinata maniera ed entro un determinato termine, ordinando in particolare la rettifica o la cancellazione di dati personali o la limitazione del trattamento", e di imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento. Devono disporre inoltre del potere di intentare un'azione o di agire in sede giudiziale contro titolari o responsabili che agiscano in violazione della direttiva, o di sottoporre all'attenzione delle competenti autorità giudiziarie (incaricate del perseguimento di reati) tali supposte violazioni (Art. 47, paragrafo 1, paragrafo 2, paragrafo 5, DPDPG). Le autorità di controllo svolgono anche un importante funzione consultiva e devono avere il diritto di

> formulare, di propria iniziativa o su richiesta, **pareri destinati al proprio parlamento nazionale e al proprio governo** …, oppure, conformemente al proprio diritto nazionale, ad altri istituzioni e organismi nonché al pubblico su questioni riguardanti la protezione dei dati personali. (Art. 47, paragrafo 3)

Le autorità sono tenute, inoltre, a pubblicare una relazione annuale sulle attività svolte, "in cui può figurare un elenco delle tipologie di violazioni notificate e di sanzioni imposte" (Art. 49).

In ogni caso, le decisioni delle autorità di controllo sono soggette a "garanzie adeguate, inclusi il ricorso giurisdizionale effettivo e il giusto processo, previste dal diritto dell'Unione e dello Stato membro conformemente alla Carta" (Art. 47, paragrafo 4).

Si deve sottolineare che la DPDPG prevede quanto segue:

> Gli Stati membri dispongono che le autorità competenti pongano in essere meccanismi efficaci per incoraggiare la segnalazione riservata di violazioni della presente direttiva. (Art. 48)

Si tratta di una previsione in linea con quelle contenute nella direttiva sul *whistleblowing* di recente adozione.[187]

[187] Direttiva del Parlamento europeo e del Consiglio sulla protezione delle persone che segnalano violazioni del diritto dell'Unione, 2019. Al momento della redazione del Manuale, il testo non risultava ancora pubblicato sulla Gazzetta Ufficiale dell'Ue, e quindi non gli era stata ancora attribuita una specifica numerazione. Tuttavia, il testo finale, come adottato dal Parlamento europeo il 16 aprile 2019, salve modifiche linguistiche e/o editoriali, è disponibile qui: https://www.europarl.europa.eu/doceo/document/TA-8-2019-0366_EN.html?redirect.

L'Art. 50 prevede un obbligo di reciproca assistenza fra le autorità di controllo degli Stati membri dell'Ue, competenti in rapporto al trattamento di dati personali disciplinato dalla DPDPG.

Inoltre, anche il Comitato europeo della protezione dei dati (CEPD), istituito dal GDPR, dispone di competenze in rapporto ai trattamenti disciplinati dalla direttiva (Art. 51). In tal senso, il Comitato può emanare linee-guida, raccomandazioni e migliori prassi su ogni materia attinente alla direttiva, nonché

> un parere per valutare l'adeguatezza del livello di protezione in un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo o in un'organizzazione internazionale, come pure per valutare se tale paese terzo, territorio, settore specifico o organizzazione internazionale non garantiscano più un livello adeguato di protezione (Art. 51(1), lettera g))

Il Comitato deve trasmettere pareri, linee-guida, raccomandazioni e migliori passi alla Commissione (e al Comitato istituito ai sensi dell'Art. 93 GDPR), e deve pubblicarli (Art. 51, paragrafo 3). La Commissione, a sua volta, deve informare il Comitato del seguito dato ai pareri, linee-guida ecc. in questione (Art. 51, paragrafo 4).

Ricorsi, responsabilità e sanzioni

Nel Capo VIII sono disciplinati ricorsi, responsabilità e sanzioni che devono trovare spazio nelle leggi nazionali di recepimento della direttiva.

In sintesi, e in linea con il GDPR, ciascun interessato deve avere il diritto di presentare un reclamo alla competente autorità di controllo se ritiene che il trattamento di dati personali che lo riguardano violi disposizioni adottate ai sensi della DPDPG (Art. 52), nonché il diritto di ottenere un'efficace tutela giudiziaria nei confronti di ogni decisione giuridicamente vincolante adottata dall'autorità di controllo nei suoi riguardi (Art. 53) e nei confronti di ogni titolare o responsabile soggetto alle norme nazionali di recepimento della DPDPG "qualora ritenga che i diritti di cui gode ai sensi delle disposizioni adottate a norma della presente direttiva siano stati violati a seguito del trattamento dei propri dati personali in violazione di tali disposizioni" (Art. 54). Inoltre, sempre in linea con il GDPR,

> l'interessato [ha] il diritto di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro, che siano debitamente costituiti secondo il diritto dello Stato membro, abbiano obiettivi statutari che siano di pubblico interesse e siano attivi nel settore della tutela dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di proporre il reclamo per suo conto e di esercitare per suo conto i diritti di cui agli articoli 52, 53 e 54. (Art. 55)

Gli interessati hanno il diritto di ottenere un risarcimento in caso di danni materiali o morali provocati da trattamenti in violazione della DPDPG (Art. 56).

Infine, gli Stati membri devono prevedere sanzioni "efficaci, proporzionate e dissuasive" in caso di violazioni della DPDPG (Art. 57).

Recepimento ritardato

Si è già osservato nei paragrafi precedenti che non tutti i trattamenti di dati personali per scopi giudiziari o di polizia o per finalità di sicurezza pubblica devono essere

immediatamente conformi alla DPDPG o alle disposizioni nazionali di recepimento di quest'ultima. La direttiva contiene infatti numerose previsioni che consentono l'allineamento alla direttiva stessa di alcuni strumenti e trattamenti solo entro un termine successivo, e in alcuni casi senza fissare alcun termine specifico. Tali disposizioni di "recepimento ritardato" riguardano "atti giuridici" dell'Ue, trattati fra Stati membri dell'Ue e paesi terzi o organizzazioni internazionali (fra cui l'Interpol), e particolari sistemi di trattamento automatizzato degli Stati membri nel settore del diritto penale e della sicurezza pubblica.

Recepimento ritardato con riguardo ad atti giuridici dell'Ue

L'Art. 60 della DPDPG prevede quanto segue, con riguardo ai circa 123 strumenti Ue ("atti giuridici" di varia tipologia) nel settore giustizia e affari interni (GAI)[188]:

> Rimangono impregiudicate le disposizioni specifiche per la protezione dei dati personali contenute in atti giuridici dell'Unione che sono entrati in vigore il o anteriormente al 6 maggio 2016 nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia, che disciplinano il trattamento tra Stati membri e l'accesso delle autorità nazionali designate ai sistemi d'informazione istituiti ai sensi dei trattati, nell'ambito di applicazione della presente direttiva.

Tuttavia, l'Art. 62, paragrafo 6, della direttiva specifica che, entro il 6 maggio 2019, la Commissione deve aver sottoposto a riesame:

> gli altri atti giuridici [diversi, ossia, dalla DPDPG stessa] adottati dall'Unione che disciplinano il trattamento da parte delle autorità competenti per le finalità di cui all'articolo 1, paragrafo 1, in particolare quelli di cui all'articolo 60, al fine di valutare la necessità di allinearli alla presente direttiva e formulare, ove opportuno, le proposte necessarie per modificarli in modo da garantire un approccio coerente alla protezione dei dati personali nell'ambito della presente direttiva.

Ne consegue che non si richiede che i 123 "atti giuridici" di cui sopra siano allineati alla DPDPG entro il 6 maggio 2019, bensì soltanto che siano sottoposti a *riesame* entro tale data al fine di *proporre* eventuali modifiche ove necessario. Non è previsto alcun termine per apportare tali necessarie modifiche, né per la presentazione delle specifiche proposte riferite ai singoli strumenti.[189]

Nel frattempo, secondo quanto prevede l'Art. 60, le norme di protezione dati contenute nei 123 atti giuridici di cui sopra restano in vigore senza alcuna modifica e possono quindi legititmare i trasferimenti di dati personali nel settore del diritto penale e della sicurezza pubblica anche se non soddisfano i criteri fissati nella DPDPG – purché siano rispettati i **tre requisiti preliminari** previsti per tali trasferimenti: ossia, che il trasferimento sia (dal punto di vista dell'autorità Ue che procede al trasferimento stesso) "necessario" per uno scopo di natura penale o connesso alla sicurezza pubblica; che il trasferimento avvenga verso un'autorità del paese terzo competente in tali settori (a meno che l'autorità in questione operi in modo inefficace, tardivo o, ancor peggio, in violazione di diritti umani); infine, se i dati trasmessi erano stati ottenuti inizialmente da un altro Stato membro, che quest'ultimo Stato membro abbia autorizzato il trasferimento (ovvero, in casi urgenti, ne sia stato almeno informato). Tutto ciò a

[188] V. Emilio De Capitani, op.cit., (nota 139, *supra*).

[189] All'atto dell'ultima revisione di questa prima edizione del Manuale (maggio 2019) non erano state ancora formulate proposte in merito dalla Commissione.

condizione che lo strumento giuridico pertinente contenga garanzie "adeguate" in materia di protezione dei dati, oppure che (se tali garanzie non sono contemplate) "l'autorità competente dell'Ue che trasferisce i dati determin[i] che diritti e libertà fondamentali dell'interessato non prevalgono sull'interesse pubblico al trasferimento".

È essenziale sottolineare che, in conformità del nuovo principio di "responsabilizzazione", le valutazioni compiute dal soggetto che trasferisce i dati (sulla presenza di garanzie "adeguate" nello strumento giuridico in esame, ovvero sulla prevalenza dell'interesse pubblico al trasferimento rispetto all'esigenza di tutelare diritti e libertà fondamentali dell'interessato e sulle relative motivazioni) devono essere documentate e, su richiesta, messe a disposizione del Garante europeo per la protezione dei dati (e della Corte di giustizia).

Ovviamente, tutti i RPD che operano all'interno di agenzie, organi o enti dell'Ue giocheranno un ruolo fondamentale in questa partita: in primo luogo, segnalando all'ente l'esigenza di effettuare tali valutazioni, e in secondo luogo verificando che le valutazioni siano svolte in modo corretto e consultando, se necessario, il Garante europeo della protezione dei dati in caso di disaccordi o problematiche interne all'ente con riguardo a tali materie.

Recepimento ritardato con riguardo a trattati fra Stati membri dell'Ue e paesi terzi o organizzazioni internazionali

Abbiamo già rilevato come l'Art. 61 preveda quanto segue:

> Restano in vigore, fino alla loro modifica, sostituzione o revoca, gli accordi internazionali relativi al trasferimento di dati personali verso paesi terzi o organizzazioni internazionali che sono stati conclusi dagli Stati membri anteriormente al 6 maggio 2016 e che sono conformi al diritto dell'Unione applicabile anteriormente a tale data.

Pertanto, i trasferimenti svolti sulla base di trattati stipulati con paesi terzi o organizzazioni internazionali precedentemente al mese di maggio 2016 possono proseguire, per il momento, a condizione che siano soddisfatti i tre requisiti preliminari fissati in merito nella DPDPG: ossia, che il trasferimento sia (dal punto di vista dell'autorità che procede al trasferimento stesso) "necessario" per uno scopo di natura penale o connesso alla sicurezza pubblica; che il trasferimento avvenga verso un'autorità del paese terzo competente in tali settori (a meno che l'autorità in questione operi in modo inefficace, tardivo o, ancor peggio, in violazione di diritti umani); infine, se i dati trasmessi erano stati ottenuti inizialmente da un altro Stato membro, che quest'ultimo Stato membro abbia autorizzato il trasferimento (ovvero, in casi urgenti, ne sia stato almeno informato). Tutto ciò a condizione che lo strumento giuridico pertinente contenga garanzie "adeguate" in materia di protezione dei dati, oppure che (se tali garanzie non sono contemplate) "l'autorità competente che trasferisce i dati determin[i] che diritti e libertà fondamentali dell'interessato non prevalgono sull'interesse pubblico al trasferimento".

Si deve sottolineare nuovamente che, in conformità del nuovo principio di "responsabilizzazione", le valutazioni compiute dall'autorità che trasferisce i dati (sulla presenza di garanzie "adeguate" nel trattato in esame, ovvero sulla conformità di tale

trattato alle disposizioni contenute nel diritto dell'Ue vigente precedentemente al mese di maggio 2016, ovvero ancora sulla prevalenza dell'interesse pubblico al trasferimento rispetto all'esigenza di tutelare diritti e libertà fondamentali dell'interessato e sulle relative motivazioni) devono essere documentate e, su richiesta, messe a disposizione dell'autorità di controllo (e delle autorità giudiziarie).

Anche in questo caso, sarà essenziale il ruolo del RPD operante presso la specifica autorità competente dello Stato membro.

Recepimento ritardato con riguardo a particolari sistemi di trattamento automatizzato degli Stati membri nel settore del diritto penale e della sicurezza pubblica

Il primo paragrafo dell'Art. 63, dedicato specificamente al recepimento della DPDPG, prevede quanto segue[190]:

> Gli Stati membri adottano e pubblicano, entro il 6 maggio 2018, le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva. Essi comunicano immediatamente alla Commissione il testo di tali disposizioni. Essi applicano tali disposizioni a decorrere dal 6 maggio 2018.

Ne consegue che, in linea di principio, le "disposizioni legislative, regolamentari e amministrative" di cui sopra avrebbero dovuto essere allineate alla DPDPG entro tale termine.

Tuttavia, lo stesso articolo prevede la seguente eccezione condizionata, al paragrafo immediatamente successivo:

> In deroga al paragrafo 1, uno Stato membro può disporre che, in via eccezionale, qualora ciò comporti sforzi sproporzionati, i sistemi di trattamento automatizzato istituiti anteriormente al 6 maggio 2016 siano resi conformi all'articolo 25, paragrafo 1, entro il 6 maggio 2023.

Il terzo paragrafo dell'articolo consente un'ulteriore estensione dei termini di recepimento, salvo il rispetto di alcune condizioni aggiuntive:

> In deroga ai paragrafi 1 e 2 del presente articolo, uno Stato membro può, in circostanze eccezionali, rendere un sistema di trattamento automatizzato di cui al paragrafo 2 del presente articolo conforme all'articolo 25, paragrafo 1, entro un termine specificato dopo il termine di cui al paragrafo 2 del presente articolo, qualora ciò causi altrimenti gravi difficoltà per il funzionamento di tale particolare sistema di trattamento automatizzato. Lo Stato membro in questione comunica alla Commissione i motivi di tali gravi difficoltà e i motivi del termine specificato entro il quale rende tale particolare sistema di trattamento automatizzato conforme all'articolo 25, paragrafo 1. Il termine specificato non supera in ogni caso il 6 maggio 2026.

Tutto ciò significa che la piena applicazione di tutti i requisiti fissati nella DPDPG, compresi in particolare quelli connessi ai trasferimenti verso paesi terzi e organizzazioni

[190] Il quarto e ultimo paragrafo dell'articolo in questione prevede che "Gli Stati membri comunicano alla Commissione il testo delle disposizioni fondamentali di diritto interno che adottano nel settore disciplinato dalla presente direttiva". La disposizione più specifica contenuta nel primo paragrafo evidenzia come la piena applicazione della DPDPG scaturisca da un esercizio scaglionato lungo un arco temporale esteso piuttosto che da un atto singolo di recepimento.

internazionali, necessiterà di tempi prolungati.

Tuttavia, nel frattempo è opportuno ricordare che in base alla direttiva (e diversamente da quanto avveniva in vigenza della Decisione quadro del Consiglio, ora abrogata) le norme e le attività di Ue e Stati membri in materia penale e di sicurezza pubblica sono soggette a controllo giurisdizionale. Ciò comprende in ultima analisi la verifica della conformità alla DPDPG di tali norme e attività – e, quindi, anche del rispetto dei requisiti sopra ricordati: cioè se un trattato contenga garanzie "adeguate" in tema di protezione dei dati o sia conforme al diritto dell'Ue vigente prima del mese di maggio 2016, e se nel caso specifico l'interesse pubblico al trasferimento prevalga effettivamente sull'esigenza di tutelare i diritti e le libertà fondamentali degli interessati, nonché, in caso di ritardi nell'allineamento fra tali norme e attività e le previsioni della DPDPG, se siano rispettate le specifiche condizioni che giustificano ritardi nel pieno recepimento della direttiva stessa (vedi paragrafi precedenti).

1.4.4 Nuovi strumenti di protezione dati nel settore della Politica Estera e di Sicurezza Comune (PESC)

Per citare quanto rappresentato dalla Commissione europea[191],

> Il Trattato di Lisbona del 2009 ha contribuito in misura considerevole a rafforzare le attività dell'Unione nel settore delle azioni esterne. In primo luogo, ha consentito di introdurre la figura dell'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza. (…)
>
> In secondo luogo, il Trattato ha creato il Servizio europeo di azione esterna (EEAS). Operativo dal 2011, esso rappresenta in sostanza il nuovo servizio diplomatico dell'Ue incaricato di supportare l'Alto rappresentante nella conduzione della politica estera dell'Ue. In particolare, l'EEAS gestisce la rete delle 141 delegazioni dell'Unione europea in tutto il mondo.
>
> L'EEAS ha il compito di garantire la coerenza e il coordinamento dell'azione esterna dell'Ue, attraverso proposte di cui garantisce l'attuazione previa approvazione da parte del Consiglio europeo. (…)
>
> Affianca l'EEAS un nuovo servizio della Commissione, il servizio per gli strumenti di politica estera (FPI), creato per gestire le spese operative.
>
> Attualmente, sotto la direzione dell'Alto rappresentante, e in stretta cooperazione con l'EEAS e le delegazioni dell'Ue, il FPI ha il compito di … implementare il bilancio di previsione concernente la Politica Estera e di Sicurezza Comune (PESC) [oltre a numerosi altri strumenti e azioni] (…)[192]
>
> Il bilancio di previsione per l'ampia gamma di attività gestite dal FPI ammonta a 733 milioni di Euro (2014).

Le attività dell'Alto rappresentante, dell'EEAS e del personale del FPI comportano

[191] Si veda: https://ec.europa.eu/fpi/about-fpi_en

[192] Un elenco contenente rinvii ai singoli strumenti e alle singole azioni è rinvenibile nella pagina web citata nella nota precedente.

spesso il trattamento di dati personali, per esempio in rapporto all'irrogazione di sanzioni individuali o al congelamento di beni patrimoniali.[193]

Tuttavia, tali trattamenti non sono disciplinati dalle stesse norme del trattato Ue applicabili ai trattamenti svolti da soggetti che ricadono nel campo di applicazione del RGPD o della DPDPG, né dalle altre istituzioni dell'Ue. Tali ultimi trattamenti sono infatti ricompresi nel principio generale a garanzia della protezione dei dati fissato dall'Art. 16 del TFUE:

Articolo 16

1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti.

Quanto sopra non si applica però al trattamento di dati personali svolto dagli organismi PESC sopra ricordati, in forza di quanto previsto all'ultimo periodo dell'Art. 16 TFUE:

Le norme adottate sulla base del presente Articolo fanno salve le norme specifiche di cui all'Articolo 39 del TUE.

Quest'ultimo articolo del Trattato sull'Unione europea prevede quanto segue:

Articolo 39

Conformemente all'articolo 16 del trattato sul funzionamento dell'Unione europea e in deroga al paragrafo 2 di detto articolo, il Consiglio adotta una decisione che stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del presente capo, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti.

Non è questa la sede per analizzare ulteriormente le tematiche sopra accennate[194]. Ci limiteremo a osservare che nel settore della PESC trova applicazione il regolamento sui trattamenti di dati personali da parte delle istituzioni dell'Ue (Regolamento 2018/1725, vedi *infra*), ma solo in misura limitata. Inoltre, per individuare le specifiche norme di protezione dati applicabili ai singoli trattamenti svolti nel settore della PESC – nonché l'autorità di controllo competente e l'ambito di tale competenza, e l'eventuale obbligo di designare un RPD – è necessario conoscere la specifica decisione del Consiglio che ha

[193] Si vedano i pareri e le osservazioni del GEPD sul punto, elencati qui: https://edps.europa.eu/data-protection/our-work/subjects/common-foreign-and-security-policy_en

[194] Per approfondimenti ulteriori, si vedano:
- La lettera del GEPD del 23 luglio 2007 alla Presidenza della Commissione IGC sulla protezione dei dati nel trattato di riforma (denominazione attribuita al Trattato di Lisbona durante la fase di redazione);
- EDPS, Joint Opinion on the notifications for Prior Checking received from the Data Protection Officer of the Council of the European Union regarding the processing of personal data for restrictive measures with regard to the freezing of assets, Brussels, 07 May 2014 (2012-0724, 2012-0725, 2012-0726), p. 10, disponibile qui: https://edps.europa.eu/sites/edp/files/publication/14-05-07_processing_personal_data_council_en.pdf

previsto lo specifico trattamento in questione.

1.4.5. La protezione dei dati nelle istituzioni dell'Ue: un nuovo regolamento

Nel paragrafo 1.3.6. si è detto che il primo strumento giuridico dell'Ue relativo al trattamento di dati personali da parte delle istituzioni dell'Ue, ossia il Regolamento 45/2001, è stato sostituito dal Regolamento (Ue) 2018/1725 entrato in vigore l'11 dicembre 2018[195] – seppure con alcune eccezioni e alcune estensioni dei termini di implementazione, come illustrato nei paragrafi seguenti.

Due regimi giuridici

A parte le eccezioni ed estensioni suddette, il Regolamento 2018/1725 crea in effetti due regimi distinti in materia di protezione dei dati: uno applicabile a tutte le istituzioni e gli organi dell'Ue che non si occupano della cooperazione di polizia e giudiziaria, ed un diverso regime applicabile alle istituzioni e agli organi dell'Ue che sono invece coinvolti in tali attività di cooperazione (v. Art. 2, paragrafi 1 e 2).

- **La disciplina di protezione dati applicabile alle istituzioni dell'Ue che non si occupano di cooperazione di polizia e giudiziaria:**

Questa disciplina, contenuta nei Capi I-VIII del nuovo regolamento, è sovrapponibile in buona parte a quella introdotta dal RGPD per i trattamenti che ricadono nel rispettivo campo di applicazione. Pertanto, il Regolamento 2018/1725 contiene – analogamente al RGPD – il nuovo principio di "responsabilizzazione" (Art. 4, paragrafo 2); si veda anche l'Art. 26) e fissa gli obblighi di titolari e responsabili del trattamento (Capo IV) sostanzialmente in termini identici a quelli applicabili ai titolari e responsabili soggetti al RGPD.

Nello specifico, il Capo IV contiene disposizioni sul principio di "protezione dei dati per impostazione predefinita e fin dalla fase di progettazione" (Art. 27); sulle misure da adottare con riguardo a "co-titolari" (Art. 28), responsabili del trattamento (Art. 29) e soggetti autorizzati al trattamento dal titolare o dal responsabile (Art. 30), sull'obbligo di tenuta di registri dettagliati dei trattamenti (connesso al principio di responsabilizzazione) (Art. 31), sulla sicurezza dei trattamenti (Art. 33), la notifica al GEPD di violazioni dei dati (essendo il GEPD l'autorità di controllo competente con riguardo alle istituzioni e agli organismi dell'Ue) (Art. 34), e sulla comunicazione di violazioni dei dati agli interessati (Art. 35) – tutto questo sulla falsariga del RGPD.

Il regolamento 2018/1725, come il suo predecessore, ossia il regolamento 45/2001 (v. paragrafo 1.3.6) impone la designazione di un Responsabile della protezione dei dati da parte di ogni istituzione o organismo dell'Ue (Art. 43); anche tale previsione corrisponde a quanto dispone il RGPD con riguardo ai titolari del settore pubblico. Anche le norme concernenti la posizione del RPD (Art. 44) e i compiti del RPD (Art. 45) sono allineate a

[195] REGOLAMENTO (UE) 2018/1725 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 23 ottobre 2018 sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE, disponibile qui: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725

quelle del RGPD, con alcune previsioni ulteriori concernenti l'accesso al RPD (possibile a chiunque) e la tutela accordata in questi casi (Art. 44, paragrafo 7) nonché sulla durata dell'incarico di RPD (Art. 45, paragrafo 8). Quanto ai compiti del RPD, nel regolamento 2018/1725 si rinviene una disposizione più cogente rispetto al RGPD poiché il RPD "deve garantire in modo indipendente l'applicazione interna del presente Regolamento" (Art. 45(1), lettera b)). [196]

Anche il regolamento 2018/1725 impone di condurre una valutazione di impatto sulla protezione dei dati (DPIA) nelle stesse situazioni previste dal RGPD – ossia, con riguardo a trattamenti "che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (Art. 39) – nonché l'obbligo di "consultazione preventiva" del GEPD al verificarsi di circostanze analoghe a quelle che disciplinano la consultazione preventiva della competente autorità di controllo in base al RGPD – ossia, qualora la DPIA indichi che i rischi suddetti non sono mitigabili in misura sufficiente (Art. 40). [L'ultimo periodo nel testo dell'Art. 40 aggiunge poi, assai opportunamente, che "Il titolare si consulta con il responsabile della protezione dei dati sull'esigenza di effettuare una consultazione preventiva" – il che è ovviamente indicato anche in rapporto ai trattamenti disciplinati dal RGPD.]

In termini sostanziali, il regolamento 2018/1725 si fonda sulle stesse definizioni (Art. 3) e gli stessi principi cardine (Art. 4) del RGPD, e contiene di fatto le stesse previsioni in materia, per esempio, di consenso e altre basi giuridiche per il trattamento di dati sensibili e ordinari (v. Artt. 5-13). Tuttavia, vi si rinvengono alcune disposizioni più specifiche quanto ai "trattamenti [ulteriori] compatibili" (Art. 6) e alla trasmissione di dati personali a destinatari in Paesi membri (Art. 9)[197] nonché ai diritti degli interessati (Artt. 14-24) anche con riguardo a decisioni esclusivamente automatizzate e profilazione (Art. 24).

Il regolamento in esame consente sostanzialmente le stesse limitazioni ai diritti degli interessati e all'obbligo di comunicare agli interessati una violazione dei dati (Art. 25, paragrafo 1), estendendo però tali limitazioni anche all'obbligo di garantire la riservatezza delle comunicazioni elettroniche (v. *infra*) e, soprattutto, prevedendo norme più specifiche sulle disposizioni che devono figurare in qualsiasi "atto giuridico o norma interna" in cui siano fissate le limitazioni suddette (v. Art. 25, paragrafo 2). Inoltre, è richiesta la consultazione del GEPD su ogni proposta normativa in materia (Art. 41, paragrafo 2), il che rappresenta una garanzia significativa al fine di assicurare che tali limitaziaoni siano "necessarie e proporzionate…in una società democratica".

Il regolamento 2018/1725 contiene una sezione specifica (Capo IV, sezione 3) sulla riservatezza delle comunicazioni elettroniche. Vi si prevede che

[196] Si tratta di una previsione più cogente perché, nonostante il RGPD stabilisca che "il titolare e il responsabile assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti" e che "[il RPD] non è rimosso o penalizzato dal titolare o dal responsabile per l'esecuzione dei propri compiti" (Art. 38, paragrafo 3, RGPD), e ciò possa in concreto garantire che il RPD sia in grado di agire "in modo indipendente", il RGPD prevede che il RPD debba "sorvegliare l'osservanza del [RGPD e delle altre norme pertinenti]" e "informare e consigliare" titolare e dipendenti di quest'ultimo, nonché eventuali responsabili, degli obblighi loro incombenti (Art. 39(1), lettere b) e (a), rispettivamente): quindi, il RGPD non impone al RPD di "assicurare" l'osservanza interna delle norme, poiché di tale osservanza è giuridicamente responsabile il titolare.

[197] V. paragrafo 1.4.6, *infra*.

> Le istituzioni e gli organi dell'Unione garantiscono la riservatezza delle comunicazioni elettroniche, in particolare proteggendo le proprie reti di comunicazione elettronica (Art. 36).

e che

> Le istituzioni e gli organi dell'Unione tutelano le informazioni trasmesse all'apparecchiatura terminale degli utenti, conservate nell'apparecchiatura terminale degli utenti, relative all'apparecchiatura terminale degli utenti, elaborate dall'apparecchiatura terminale degli utenti e raccolte dall'apparecchiatura terminale degli utenti che accede ai loro siti web e alle applicazioni per dispositivi mobili a disposizione del pubblico, in ottemperanza all'articolo 5, paragrafo 3, della direttiva 2002/58/CE [la direttiva e-privacy, di cui al paragrafo 1.3.3., *supra*] (Art. 37)

L'ultimo articolo di tale sezione riguarda gli elenchi di utenti come definiti all'Art. 3, paragrafo 24, ossia ogni

> elenco di utenti accessibile al pubblico o elenco interno di utenti disponibile in un'istituzione od organo dell'Unione o condiviso tra istituzioni e organi dell'Unione, in formato cartaceo o elettronico.

Al riguardo, l'Art. 38 prevede che i dati personali figuranti in tali elenchi devono essere "limitati a quanto è strettamente necessario per i fini specifici dell'elenco" (Art. 38, paragrafo 1), e che le istituzioni e gli organismi

> prendono le misure necessarie per impedire che i dati personali contenuti in tali elenchi siano utilizzati a fini di diffusione commerciale diretta, indipendentemente dal fatto che gli elenchi siano o meno accessibili al pubblico.

Le norme di questa sezione rispecchiano alcune di quelle contenute nella direttiva e-privacy, di cui abbiamo parlato nella sezione 1.3.3. del Manuale.

Le norme che disciplinano i trasferimenti di dati verso paesi terzi o organizzazioni internazionali sono contenute nel Capo V del regolamento 2018/1725 e presentano la stessa struttura di quelle contenute nel RGPD. In sintesi, tali trasferimenti sono consentiti esclusivamente:

- sulla scorta di una decisione di adeguatezza adottata dalla Commissione europea ai sensi del RGPD; oppure

- se sono fornite garanzie adeguate attraverso

> uno strumento giuridicamente vincolante e avente efficacia esecutiva fra autorità o soggetti pubblici;
>
> clausole-tipo di protezione dei dati adottate dalla Commissione;
>
> clausole-tipo di protezione dei dati adottate dal GEPD e approvate dalla Commissione;
>
> con riguardo a trasferimenti verso un responsabile che non sia un organismo o un'istituzione dell'Ue: norme vincolanti d'impresa (BCR), codici di condotta o certificazioni emesse ai sensi del RGPD; oppure

salva l'autorizzazione del GEPD:

- clausole contrattuali fra i soggetti coinvolti nel trasferimento; oppure

- disposizioni in materia di protezione dei dati inserite in strumenti (accordi) amministrativi fra autorità o soggetti pubblici.

(Art. 48)

Il regolamento contiene anche la stessa disposizione del RGPD in base alla quale:

> Le sentenze di un'autorità giurisdizionale e le decisioni di un'autorità amministrativa di un paese terzo che dispongono il trasferimento o la comunicazione di dati personali da parte di un titolare del trattamento o di un responsabile del trattamento possono essere riconosciute o assumere qualsivoglia carattere esecutivo soltanto se basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione (Art. 49)

Infine, sempre sul punto, l'Art. 50 del regolamento prevede la possibilità di trasferire dati sulla base di "deroghe in situazioni specifiche", analoghe a quelle contenute nel RGPD – quindi, se l'interessato ha "acconsentito esplicitamente" al trasferimento (Art. 50(1), lettera a)) o se il trasferimento è "necessario" in un contesto contrattuale (Art. 50(1), lettera b) e lettera c)), per importanti ragioni di interesse pubblico riconosciute dal diritto dell'Unione (Art. 50(1), lettera d), in combinato disposto con l'Art. 50, paragrafo 3), al fine di accertare, difendere o esercitare un diritto in sede giudiziaria (Art. 50(1), lettera e)) o di tutelare gli interessi vitali dell'interessato o di terzi ove l'interessato sia nell'incapacità fisica o giuridica di prestare il consenso (Art. 50(1), lettera f)) oppure se il trasferimento è effettuato a partire da un registro pubblicamente accessibile (purché siano rispettate le condizioni che ne disciplinano l'accesso) (Art. 50(1), lettera g)).

Come già il RGPD nei riguardi delle autorità pubbliche, il regolamento 2018/1725 dispone che le prime tre fra le deroghe di cui sopra (consenso esplicito dell'interessato, contesti contrattuali) "non si applicano alle attività svolte dalle istituzioni e dagli organi dell'Unione nell'esercizio dei pubblici poteri" (Art. 50, paragrafo 2).

Nel Capo VI del regolamento sono disciplinati l'istituzione, le norme, la posizione, i compiti e i poteri del GEPD. In estrema sintesi, il GEPD svolge con riguardo al trattamento di dati personali da parte di istituzioni e organi dell'Ue le stesse funzioni delle autorità di controllo istituite negli Stati membri (o nelle articolazioni regionali degli Stati membri) ai sensi del RGPD con riguardo ai trattamenti di dati personali svolti dalle rispettive autorità pubbliche nazionali per le quali risultano essere competenti.

Il Capo VII riguarda la cooperazione e la supervisione coordinata fra il GEPD e le autorità nazionali di controllo. Analogamente al RGPD, il regolamento 2018/1725 promuove la cooperazione con paesi terzi e organizzazioni internazionali ai fini della protezione dei dati personali (Art. 51).[198]

Infine, il Capo VIII disciplina ricorsi giurisdizionali, responsabilità e sanzioni, ancora una

[198] È singolare che la disposizione in materia (Art. 50) figuri (come nel caso del RGPD) nel Capo dedicato ai trasferimenti di dati, anziché in quello relativo a compiti e poteri delle autorità di controllo.

volta in termini analoghi a quelli fissati nel RGPD. Ci limitiamo a osservare che un interessato i cui dati personali sono o sono stati trattati da un'istituzione o un organo dell'Ue ha il diritto di presentare un reclamo presso il GEPD (Art. 63) esattamente come gli interessati hanno, in base al RGPD, il diritto di presentare un reclamo alla competente autorità nazionale di controllo; inoltre, e sempre sulla falsariga del RGPD, ogni interessato ha diritto al risarcimento di danni materiali e immateriali causati da violazioni del Regolamento (Art. 65). In questi casi l'interessato può farsi rappresentare da organismi no-profit attivi nel settore della protezione dei dati (Art. 67), e sul punto questo regolamento aggiunge una disposizione ulteriore in merito ai reclami presentati dal personale delle istituzioni o degli organi dell'Ue (Art. 68). Viceversa, ogni funzionario dell'Ue che ometta di rispettare gli obblighi fissati dal regolamento è passibile di azioni disciplinari (Art. 69).

La Corte di giustizia dell'Ue è competente per ogni controversia concernente il regolamento 2018/1725, anche per quanto riguarda eventuali risarcimenti (Art. 64). Il GEPD ha il potere di irrogare sanzioni amministrative pecuniarie alle istituzioni e agli organi dell'Unione che violino le disposizioni del Regolamento in questione (Art. 66) – anche se l'entità di tali sanzioni è considerevolmente inferiore a quella prevista nel RGPD.[199]

Tenuto conto che l'architettura generale delle disposizioni in materia di protezione dei dati contenute nel Regolamento 2018/1725 è sovrapponibile, in buona parte, a quella del RGPD, le linee-guida e i pareri, spesso dettagliati e ricchi di indicazioni concrete, che il GEPD emana nei confronti di istituzioni e organi dell'Ue soggetti a tale Regolamento avranno rilevanza diretta anche per i responsabili e titolari che trattano dati personali ai sensi del RGPD, soprattutto nel settore pubblico. Pertanto, è opportuno che ogni RPD operante presso uno di tali titolari studi con attenzione le linee-guida e i pareri suddetti – naturalmente in aggiunta alle linee-guida e ai pareri del Comitato europeo per la protezione dei dati, di cui fa parte anche il GEPD. CEPD e GEPD contribuiscono reciprocamente alla definizione di tali strumenti.

- **La disciplina di protezione dati applicabile alle istituzioni dell'Ue che si occupano di cooperazione di polizia e giudiziaria:**

Osservazioni generali

Si è rilevato in precedenza che il Regolamento 2018/1725 crea un regime distinto in materia di protezione dei dati per quelle istituzioni e quegli organi dell'Ue che si

[199] L'importo massimo delle sanzioni pecuniarie che il GEPD può irrogare a istituzioni e organi dell'Ue in caso di inosservanza del regolamento 2018/1725 è pari, rispettivamente, a € 25.000 per singola violazione fino a un totale di € 250.000 annui per alcune violazioni, e a € 50.000 fino a un totale di €500.000 annui per altre violazioni (v. Art. 66, paragrafi 2 e 3). Si confrontino i valori previsti nel caso del RGPD: fino a € 10 milioni o, in caso di imprese (soggetti privati), fino al 2% del fatturato annuo mondiale totale, se più elevato, per alcune violazioni, e fino a € 20 milioni o, in caso di imprese, fino al 4% del fatturato annuo mondiale globale, se più elevato, per altre violazioni (Art. 83, paragrafi 4 e 5). Tuttavia, il RGPD permette agli Stati membri di ridurre tali importi ovvero di escludere la sanzionabilità di soggetti e autorità pubbliche nel rispettivo territorio (Art. 83, paragrafo 7), anche se tali autorità, pur esenti da sanzioni amministrative pecuniarie o soggette a sanzioni ridotte, restano in ogni caso soggette ai poteri della competente autorità di controllo ai sensi dell'Art. 58, paragrafo 2, del RGPD.

occupano di cooperazione di polizia e giudiziaria – ossia partecipano ad "attività che ricadono nel campo di applicazione del Capo 4 o del Capo 5 del Titolo V della Parte terza del TFUE". Tale distinto regime è disciplinato al Capo IX del Regolamento, comprendente gli articoli da 70 a 95, mentre l'Art. 2, paragrafo 2, chiarisce che valgono comunque le definizioni fissate all'Art. 3 del suddetto Regolamento. [200]

Il regime specifico in questione disciplina il trattamento di "dati personali operativi" da parte delle competenti istituzioni o dei competenti organi dell'Ue. I dati suddetti sono definiti come segue all'Art. 3, paragrafo 2:

> tutti i dati personali trattati da organi o organismi dell'Unione nell'esercizio di attività rientranti nell'ambito di applicazione della parte terza, titolo V, capo 4 o capo 5, TFUE per conseguire gli obiettivi ed eseguire i compiti stabiliti negli atti giuridici che li istituiscono

In sintesi, il trattamento di dati personali operativi è soggetto allo speciale regime giuridico fissato nel Capo IX, mentre il trattamento di tutti i dati personali "non operativi" – come i dati relativi al personale delle istituzioni o degli organi suddetti – resta soggetto al regime generale prima descritto con riguardo ai Capi precedenti del Regolamento 2018/1725.

Si è già rilevato in proposito che le norme fissate nel regime generale di protezione dati sono allineate in misura considerevole a quelle del RGPD. Analogamente, le norme di cui al Capo IX del Regolamento 2018/1725 sono spesso assimilabili a quelle contenute nella DPDPG di cui al paragrafo 1.4.3 *supra* – ovvero a quelle contenute sia in tale ultima direttiva sia nel RGPD e nel regime generale di protezione dati definito nel Regolamento 2018/1725; tuttavia, il Capo IX non è sovrapponibile alla DPDPG nella stessa misura in cui le norme del regime generale dello stesso Regolamento sono sovrapponibili a quelle del RGPD. Si tratta di tematiche spesso complesse.[201]

Poiché il presente Manuale è destinato ai RPD che operano presso soggetti pubblici negli Stati membri, non è opportuno analizzare in questa sede le divergenze o corrispondenze fra le norme del Capo IX e quelle contenute nelle precedenti sezioni del Regolamento 2018/1725 nonché negli strumenti generali di protezione dati dell'Ue (il RGPD e la DPDPG). Vale la pena però di esaminare due questioni particolari, come illustrate nei paragrafi seguenti.

Diritti, controllo e attuazione:

Il Capo IX non contiene alcuna disposizione sul diritto dell'interessato di ottenere un

[200] Per quanto concerne l'applicabilità dei Capi VII e VIII del Regolamento in questione ai trattamenti disciplinati dal Capo IX, si veda *infra* alla voce "Diritti, controllo e attuazione".

[201] Un solo esempio: strettamente connesso al nuovo principio di "responsabilizzazione" che si applica a tutti gli strumenti moderni in materia di protezione dati nell'Ue, è l'obbligo dei titolari di tenere registri dei trattamenti e registrazioni. Tuttavia, il RGPD e le norme contenute nel regime generale di cui al Regolamento 2018/1725 prevedono la tenuta di registri dettagliati di tutti i trattamenti (Art. 30 RGPD; Art. 31 del Regolamento 2018/1725), ma non impongono la tenuta di registrazioni. La DPDPG prevede la tenuta sia di registri dettagliati, sia di registrazioni (Artt. 24 e 25), mentre il Capo IX del Regolamento 2018/1725 impone soltanto la tenuta di registrazioni con riguardo al trattamento di dati personali operativi (Art. 88) senza prescrivere la tenuta di registri dei trattamenti.

risarcimento in caso di danni provocati da trattamenti illeciti – nello specifico, ossia, contrari alle disposizioni dello stesso Capo IX – o al diritto di farsi rappresentare da un organismo no-profit, o al potere del GEPD di irrogare sanzioni amministrative pecuniarie.

È vero che nel Capo IX si menziona più volte l'obbligo per i titolari soggetti all'applicazione delle norme contenute in tale Capo di informare gli interessati del diritto di presentare reclamo al GEPD (v. Artt. 79(1), lettera d), 80, lettera f), e 81, paragrafo 2) nonché della possibilità di adire la Corte di giustizia (Art. 81, paragrafo 2). I titolari soggetti alle norme del Capo IX possono anche disporre che, in determinati casi, l'esercizio dei diritti degli interessati avvenga "tramite il GEPD" (Art. 84, paragrafo 1), ossia solo in forma indiretta. Anche in questo caso i titolari dovranno

> Informa[re] l'interessato della possibilità di esercitare i suoi diritti tramite il Garante europeo della protezione dei dati ai sensi del paragrafo 1. (Art. 84, paragrafo 2)

Il titolare deve, inoltre, mettere a disposizione del GEPD, su richiesta, le registrazioni dei trattamenti svolti (Art. 88, paragrafo 3) e notificare al GEPD le violazioni di dati personali (Art. 92, paragrafi 1 e 4).

Tuttavia, è indiscutibile che, in base all'Art. 2, paragrafo 2, il Capo del Regolamento in esame contenente le disposizioni sulla trattazione di reclami da parte del GEPD e sulla competenza della Corte di giustizia dell'Ue, nonché in materia di poteri esecutivi del GEPD anche nei casi di violazione dei dati personali (Capo VIII), e anche il Capo relativo a funzioni e poteri del GEPD in questi casi (Capo VI), non trovano applicazione al trattamento di dati operativi, essendo quest'ultimo disciplinato esclusivamente dal Capo IX.

Sembra di poter affermare, nei fatti, che il GEPD eserciterà poteri consultivi e di vigilanza anche in rapporto ai trattamenti di dati operativi da parte di istituzioni e organi dell'Ue, in base al Capo IX del Regolamento 2018/1725, e accetterà reclami degli interessati concernenti tali trattamenti. Resta da capire se ammetterà la rappresentanza da parte di ONG in questi casi, o se si spingerà fino a disporre risarcimenti o a irrogare sanzioni amministrative pecuniarie alle istituzioni e agli organi coinvolti – e se la Corte di giustizia confermerà queste modalità di esercizio dei poteri del GEPD con riguardo ai trattamenti in esame.

Casi di esclusione o di ritardata applicazione del Regolamento 2018/1725

In linea di principio, il Regolamento 2018/1725 si applica a tutti i trattamenti di dati personali svolti da istituzioni o organi dell'Unione (Art. 2, paragrafo 1), benché, come già evidenziato, esso preveda due distinti regimi giuridici. Tuttavia, esso prevede anche alcuni ambiti sottratti alla sua applicazione, e in altri casi tempi più dilatati per la sua applicazione, come vedremo nei paragrafi seguenti.

- Casi di esclusione dell'applicazione del Regolamento

L'Art. 2, paragrafo 4, prevede quanto segue:

> Il presente regolamento non si applica al trattamento dei dati personali da parte delle missioni di cui all'articolo 42, paragrafo 1, e agli articoli 43 e 44 TUE.

Le missioni e le funzioni cui tale disposizione fa riferimento sono le seguenti:

- missioni al di fuori del Ue per finalità di mantenimento della pace, prevenzione di conflitti e rafforzamento della sicurezza internazionale conformemente ai principi della Carta dell'ONU (Art. 42, paragrafo 2); e

- operazioni congiunte di disarmo, funzioni umanitarie e di salvataggio, attività di consulenza e assistenza militare, funzioni di prevenzione di conflitti e mantenimento della pace, funzioni svolte da forze di combattimento per la gestione di situazioni di crisi comprese attività di pacificazione e stabilizzazione successivamente a conflitti. (Art. 43 e Art. 44, contenente disposizioni aggiuntive)

Il secondo periodo dell'Art. 43 dispone poi che tutte le attività e le funzioni menzionate in tale articolo "possono contribuire alla lotta al terrorismo, anche attraverso il supporto fornito a paesi terzi nella lotta al terrorismo nei rispettivi territori".

- Applicazione ritardata del Regolamento

A parte i casi sopra ricordati di esclusione dal campo di applicazione del Regolamento rispetto a particolari attività che possono essere disciplinate da norme specifiche, il Regolamento prevede anche procedure per l'allineamento al Regolamento stesso delle norme di trattamento dati vigenti presso altre istituzioni e altri organi dell'Ue e specifica i termini per il riesame della normativa in questione – ma non per quanto riguarda l'attività di allineamento in quanto tale. Nello specifico, occorre esaminare in primo luogo l'Art. 2, paragrafo 3, in base al quale:

> Il presente regolamento non si applica al trattamento dei dati personali operativi da parte di Europol e della Procura europea, finché il regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio e il regolamento (UE) 2017/1939 del Consiglio[202] non saranno adattati conformemente all'articolo 98 del presente regolamento.

Inoltre, l'art. 98 prevede quanto segue:

> 1.Entro il 30 aprile 2022 la Commissione riesamina gli atti giuridici adottati a norma dei trattati che disciplinano il trattamento dei dati personali operativi da parte degli organi o degli organismi dell'Unione nell'esercizio di attività rientranti nell'ambito di applicazione della parte terza, titolo V, capo 4 o capo 5, TFUE al fine di:
>
> (a) valutarne la coerenza con la direttiva (UE) 2016/680 e con il capo IX del presente regolamento;
> (b) individuare disparità che possano ostacolare lo scambio di dati personali operativi tra gli organi o gli organismi dell'Unione nell'esercizio di attività in tali ambiti e le autorità competenti; e
>
> (c) individuare divergenze che possano dare luogo a una frammentazione giuridica della legislazione in materia di protezione dei dati nell'Unione.
>
> 2. Sulla base del riesame, allo scopo di garantire una protezione uniforme e coerente delle persone fisiche in relazione al trattamento, la Commissione può presentare a Europol e alla Procura europea adeguate proposte legislative, in particolare ai fini dell'applicazione del capo IX del presente regolamento, inclusi, se del caso, adeguamenti del capo IX del presente regolamento.

[202] Pubblicati rispettivamente in GUUE L 135 24 maggio 2016 e GUUE L 283 31 ottobre 2017.

In altri termini, i regolamenti che disciplinano l'attività dell'Europol e della Procura europea nonché di ogni altra istituzione o altro organo cui si applichi l'Art. 98 devono essere oggetto di revisione entro il 30 aprile 2022, e la Commissione potrà successivamente proporre nuove norme al fine di allineare il trattamento di dati personali da parte di tali soggetti alle disposizioni della DPDPG (v. paragrafo 1.4.3., *supra*) nonché alle norme specifiche contenute nel Capo IX del presente regolamento (v. *supra*). Tuttavia, non viene fissato alcun termine per l'adozione effettiva di tali norme, che necessita dell'intervento legiferativo del Consiglio dei Ministri e del nuovo Parlamento europeo, nonché del previo parere del GEPD e del Comitato europeo della protezione dei dati – e tutto ciò inevitabilmente richiederà tempo. In attesa degli emendamenti necessari a tale scopo, e quindi almeno per i prossimi anni, il trattamento di dati personali da parte dell'Europol e della Procura europea, nonché da parte di ogni altra istituzione o altro organo cui si applica l'Art. 98 del Regolamento 2018/1725, continuerà a essere disciplinato dalle attuali norme in materia di protezione dei dati come configurate precedentemente al 2018.

1.4.6. Trasmissione di dati personali fra enti soggetti a regimi diversi di protezione dati nell'Ue

i. I diversi regimi di protezione dei dati

Crediamo sia emerso con chiarezza da quanto precede che, nei fatti, esiste un numero consistente di regimi di protezione dati, aventi natura generale o specifica, nell'ambito dei principali strumenti dell'Unione in materia, e altri ancora ve ne sono al fuori dell'ambito unionale, talora in ambiti del tutto estranei al diritto dell'Ue – fra questi alcuni sono illustrati nei paragrafi seguenti. La definizione del regime giuridico applicabile a una particolare attività o a un determinato trattamento dipende dalla valutazione compiuta in merito a tale attività o trattamento e agli scopi perseguiti nel caso specifico, in particolare considerando se la materia sia o meno disciplinata dal diritto Ue, se l'attività o il trattamento abbia luogo nel settore pubblico o privato, se siano coinvolte istituzioni dell'Ue ovvero nazionali che si occupino di materie penali o economiche, e così via.

Regolamento generale sulla protezione dei dati

- Il regime giuridico del RGPD applicato ai trattamenti svolti da soggetti privati
- Il regime giuridico del RGPD applicato ai trattamenti svolti da soggetti pubblici che non si occupano della materia penale, della sicurezza pubblica o della sicurezza nazionale (ovvero ai soggetti operanti in tali ambiti quando non si occupano delle materie indicate) (dove l'interpretazione di "sicurezza pubblica" deve essere restrittiva).

Direttiva e-privacy/Regolamento e-privacy (proposta di)

- Le norme specifiche applicate ai fornitori di servizi di comunicazione elettronica (e in futuro ad altri fornitori come gli OTT).
- Le norme specifiche applicabili a tutti i web host (comprese le autorità pubbliche

con le rispettive pagine web) in rapporto alla riservatezza delle comunicazioni, all'utilizzo di cookies, ecc.

La direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie

- La DPDPG in quanto applicata ai soggetti pubblici ("autorità competenti") quando trattano dati personali "a fini di prevenzione, indagine, accertamento e perseguimento di reati o dell'esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica", in via prevalente o su base occasionale, a prescindere dalle altre funzioni pubbliche esercitate.

Settori sottratti all'applicazione della DPDPG (per il momento)

- Le norme contenute nei ca. 123 strumenti giuridici dell'Ue relativi alle materie un tempo denominate "giustizia e affari interni" (GAI), entrati in vigore prima del 6 maggio 2016 (e che restano applicabili anche se non sono ancora allineati alla DPDPG)
- Le norme contenute in "accordi internazionali che prevedono trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali, conclusi dagli Stati membri prima del 6 maggio 2016 e conformi al diritto dell'Unione vigente precedentemente a tale data" (anch'esse applicabili pur se non ancora conformi alla DPDPG)
- Le norme relative all'utilizzo di "sistemi di trattamento automatizzato istituiti anteriormente al 6 maggio 2016" negli Stati membri, se non sono state ancora allineate alla DPDPG in quanto ciò avrebbe comportato uno "sforzo sproporzionato".

Trattamenti di dati personali nel settore PESC

- Trattamenti svolti dall'Alto rappresentante Ue per gli affari esteri e la politica di sicurezza, dal Servizio europeo di azione esterna (EEAS) e dalle 141 delegazioni dell'Ue nel mondo, e dal servizio per gli strumenti di politica estera (FPI), nonché i trattamenti svolti dagli Stati membri in rapporto alle materie suddette (anche con riguardo all'adozione di Decisioni del Consiglio nel settore della PESC) – *i quali non sono ancora soggetti ad alcuno strumento Ue specifico in materia di protezione dei dati* [si veda però il terzo punto alla voce seguente]

Trattamenti di dati personali da parte di istituzioni o organi dell'Ue ai sensi del Regolamento 2018/1725

- Il regime giuridico in materia di protezione dati applicabile alle istituzioni o agli organi Ue che non si occupano di cooperazione di polizia e giudiziaria

- Il regime giuridico in materia di protezione dati applicabile alle istituzioni o agli organi dell'Ue che si occupano di cooperazione di polizia e giudiziaria

- I trattamenti svolti dal Segretariato del Consiglio ai fini dell'attuazione di Decisioni del Consiglio in ambito PESC, per quei limitati settori di attività concernenti la PESC che sono soggetti a norme di protezione dati, ossia al Regolamento 2018/1725

Settori sottratti all'applicazione del Regolamento 2018/1725 (per il momento)

- Trattamenti di dati personali svolti da missioni Ue per finalità di mantenimento della pace, prevenzione di conflitti e rafforzamento della sicurezza internazionale, ovvero da missioni Ue incaricate di operazioni congiunte di disarmo, funzioni umanitarie e di salvataggio, consulenza e assistenza militare, funzioni di prevenzione di conflitti e mantenimento della pace, da forze di combattimento nella gestione di situazioni di crisi, comprese attività di pacificazione, e attività di stabilizzazione successive a conflitti (anche qualora tali funzioni e attività siano connesse alla lotta al terrorismo, anche tramite il supporto fornito a paesi terzi nella lotta al terrorismo sui rispettivi territori).
- Trattamenti di dati personali svolti dall'Europol e dalla Procura europea (EPPO) e da altri "organi, uffici o agenzie dell'Unione nello svolgimento di attività che ricadono nel campo di applicazione del Capo 4 o del Capo 5 del Titolo V della Parte III del TFUE [ossia, relativi alla cooperazione di polizia o giudiziaria]", che potranno proseguire sul fondamento degli strumenti giuridici Ue relativi all'Europol e all'EPPO o, altrimenti, alla cooperazione di polizia o giudiziaria adottati anteriormente al Regolamento 2018/1725.

Sicurezza nazionale

- Trattamenti di dati personali svolti dagli Stati membri in rapporto alla sicurezza nazionale, un ambito sottratto totalmente all'intervento del diritto Ue e alla stessa Carta dei diritti fondamentali (anche se tali trattamenti sono naturalmente soggetti alla CEDU e alla giurisdizione della Corte EDU). [203]

Non è sempre facile il discrimine fra i molti e diversi regimi giuridici di cui sopra, per esempio fra le attività di polizia di contrasto della criminalità, le attività di polizia finalizzate alla tutela dell'ordine, le attività della polizia e di altre autorità miranti a garantire la "sicurezza interna", la "sicurezza pubblica" e la "sicurezza nazionale", e fra tutte queste attività e le attività dell'Ue connesse al "terrorismo"[204], alle funzioni sopra ricordate delle missioni dell'Ue, e alla "sicurezza internazionale".

Non è questa la sede opportuna per un'analisi approfondita delle differenze esistenti. Ci si limita a osservare che, quando vi sono diversi regimi giuridici applicabili alle diverse attività (attività che ricadono in più di uno dei settori sopra ricordati), magari svolte dagli stessi soggetti, sarà importante che tali soggetti in quanto titolari (e talora anche in quanto responsabili del trattamento, per esempio se supportano le attività dei primi) chiariscano autonomamente quale sia il regime giuridico applicabile ai singoli trattamenti di dati personali, e a quali dati personali si applichi tale regime, analizzando ciascuno degli specifici trattamenti in oggetto. La liceità del trattamento e la definizione

[203] La Corte EDU ha assunto numerose e importanti decisioni in questo ambito. Si veda: European Court of Human Rights Research Division, *National security and European case-law*, Council of Europe, 2013, disponibile qui:
https://www.echr.coe.int/Documents/Research_report_national_security_ENG.pdf.
Tuttavia, questa giurisprudenza non è applicabile alle istituzioni Ue con riguardo alle attività in questione.

[204] Vedi John Vervaele, *Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law?* in: Utrecht Law Review, Volume 1, Issue 1 (September 2005), disponibile qui:
http://www.utrechtlawreview.org/

degli ambiti di applicazione ovvero di esclusione dei diritti degli interessati, questione della massima rilevanza, dipendono sempre in misura sostanziale da una simile analisi chiarificatrice.

Le autorità pubbliche che partecipano a diverse attività soggette a distinti regimi giuridici in materia di protezione dei dati dovrebbero sempre operare un'attenta distinzione fra tali diverse attività, i separati trattamenti, e gli specifici dati personali utilizzati per i diversi trattamenti sia nei rispettivi registri dei trattamenti sia nelle valutazioni condotte con riguardo ai trattamenti in questione[205]. I RPD che operano presso tali soggetti pubblici avranno un ruolo-chiave da svolgere al riguardo. [206]

ii. Trasmissione di dati personali

Problematiche particolari si manifestano in tutti quei casi ove dati personali ottenuti per uno scopo specifico in base alle norme vigenti in uno dei regimi giuridici sopra ricordati siano utilizzati dallo stesso titolare per uno scopo diverso e quindi trattati secondo le regole di un diverso regime giuridico, ovvero siano trasmessi a o comunque messi a disposizione di un altro soggetto (un diverso titolare) per uno scopo diverso e quindi trattati secondo le regole di un diverso regime giuridico. [207]

Per esempio, l'ufficio istruzione di un comune raccoglie dati personali relativi agli alunni delle scuole comunali per finalità connesse alle attività educative, ai sensi del RGPD; tuttavia, l'ufficio locale di polizia potrebbe chiedere all'ufficio istruzione di accedere a (parte) di tali dati, per facilitare la gestione di episodi criminosi locali (p.es., per verificare quali alunni siano stati assenti in un giorno specifico). Il trattamento previsto dei dati degli alunni per questa seconda finalità sarebbe disciplinato dalla DPDPG (o, più precisamente, dalle disposizioni giuridiche nazionali di recepimento di tale direttiva, oltre che dalle pertinenti disposizioni del diritto penale o delle leggi di polizia). In taluni casi, le disposizioni o le norme applicabiil chiariscono quando tali comunicazioni siano consentite (p.es., solo con riguardo a determinati reati, o solo in presenza di ragionevoli sospetti nei confronti di specifici alunni, o solo su mandato dell'autorità giudiziaria). Tuttavia, spesso si tratterà di decisioni lasciate all'autorità locale che dovrà tenere conto delle norme contenute nei vari strumenti applicabili. **Il RPD di tale autorità locale avrà una funzione importante di supporto consulenziale in questa materia** (e dovrebbe consultare l'Autorità di controllo in caso di dubbi).

Il Regolamento 2018/1725 fornisce alcune indicazioni sulle comunicazioni di dati personali effettuate da un'istituzione o da un organo dell'Ue verso "destinatari stabiliti nell'Unione diversi da istituzioni e organi dell'Unione" – tipicamente si tratta di autorità

[205] V. Art. 74 del Regolamento 2018/1725, che invita a distinguere fra dati personali operativi e alla verifica della qualità di dati personali operativi, il che costituisce una buona prassi da raccomandare a tutti i titolari che svolgono attività soggette a distinti regimi giuridici in materia di protezione dei dati.
[206] V. Parte III del Manuale.
[207] Si osservi che i casi di trasmissione di dati qui esaminati non vanno confusi con la trasmissione di dati personali da parte di un soggetto a un altro soggetto nello stesso o in un altro Stato membro per la stessa finalità e all'interno dello stesso regime giuridico (vigente in UE) – per esempio, la trasmissione effettuata da un'agenzia di polizia o giudiziaria nello Stato membro A ad un'altra agenzia di polizia o giudiziaria nello Stato membro B o nello stesso Stato membro A; né vanno confusi con i trasferimenti di dati personali verso paesi terzi (soggetti a norme specifiche, anch'esse in ogni caso diverse a seconda del regime giuridico applicabile).

pubbliche dei singoli Stati membri. Istituzioni e organi dell'Ue possono comunicare dati a un soggetto stabilito in uno Stato membro che ne fa richiesta nel rispetto di alcune condizioni:

(a) il destinatario [ossia, il soggetto nello Stato membro che fa richiesta dei dati] determina che i dati sono necessari all'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di poteri autoritativi conferiti a tale destinatario; oppure
(b) il destinatario determina che la comunicazione dei dati per uno scopo specifico è necessaria nell'interesse pubblico, e il titolare [ossia, l'istituzione o l'organo dell'Ue cui viene chiesto di trasmettere i dati], ove vi siano motivi per ritenere che possano essere lesi interessi legittimi dell'interessato, determina che la trasmissione dei dati personali per tale scopo specifico è proporzionata dopo aver soppesato chiaramente i vari interessi in gioco.
(Art. 9, paragrafo 1)

Le istituzioni e gli organi dell'Ue possono inviare dati personali a soggetti stabiliti negli Stati membri senza esserne richiesti, ossia d'ufficio, se possono dimostrare

> che la trasmissione dei dati personali è necessaria e proporzionata alle finalità cui è destinata, applicando i criteri di cui al paragrafo 1, lettera a) o b).
>
> (Art. 9, paragrafo 2)

Tuttavia, vi sono numerosi elementi di cui tenere conto in materia. In primo luogo, quanto sopra vale solo per le istituzioni e gli organi dell'Ue che non trattano dati in rapporto alla cooperazione di polizia e giudiziaria – ossia, vale solo per i trattamenti e le comunicazioni di dati che ricadono nel "regime generale" fissato dal Regolamento 2018/1725 per le istituzioni e gli organi dell'Ue. Si è già rilevato al paragrafo 1.4.5 che tale regime "generale" è fortemente allineato a quello previsto nel RGPD. Nel Capo IX del Regolamento 2018/1725, che si applica ai trattamenti di dati personali "operativi" da parte di istituzioni e organi dell'Ue che partecipano alla cooperazione di polizia e giudiziaria, non esiste una disposizione analoga che disciplini le comunicazioni di dati personali a organi degli Stati membri.

In secondo luogo, le disposizioni sopra citate di cui all'Art. 9 "fanno salvi" i principi fondamentali in materia di protezione dei dati, fra cui la limitazione della finalità e la norma sulla "compatibilità" dei trattamenti (v. Art. 6 del Regolamento, che aggiunge alcune importanti condizioni al riguardo), il principio di minimizzazione, ecc.; restano impregiudicate anche le disposizioni in materia di liceità del trattamento (v. clausola di apertura dell'Art. 9, paragrafo 1) nonché le norme speciali sul trattamento di dati personali sensibili (idem).

A ogni modo, le disposizioni dell'Art. 9 del Regolamento 2018/1725 mostrano chiaramente che **ogniqualvolta si debbano trasmettere a un altro soggetto, ovvero uno stesso soggetto debba utilizzare, dati personali trattati secondo le norme previste da uno dei regimi giuridici sopra descritti, ai fini del trattamento di tali dati secondo le norme previste da un diverso regime giuridico, occorre dirimere importanti questioni connesse alla limitazione della finalità, alla pertinenza e adeguatezza dei dati, e alla liceità, necessità e proporzionalità del mutamento di scopo del trattamento**.

Sul punto, è fondamentale ricordare in prima battuta che la "trasmissione" di dati, come ogni altra forma di "comunicazione" di dati personali, compresa la "messa a disposizione" di tali dati, per esempio online, configura un trattamento (v. Art. 4, paragrafo 2, del RGPD, riprodotto in identica forma in tutti gli altri strumenti Ue in materia di protezione dei dati). In secondo luogo, si deve evidenziare come ogni "trasmissione" di dati personali fra diversi soggetti implichi sempre due elementi:

- per il soggetto che trasmette i dati, è una forma di **comunicazione** dei dati (v. *supra*); ma
- per il soggetto destinatario dei dati, configura una **raccolta** di dati personali, cioè un'attività distinta ma ricompresa nel concetto generale di "trattamento", diversa dalla "comunicazione", "trasmissione" o "messa a disposizione" di dati personali.

Qualora i due soggetti in questione, con riguardo alle attività rispettivamente connesse alla trasmissione dei dati, operino nel quadro di diversi regimi giuridici in materia di protezione dei dati, ciascuno di essi dovrebbe valutare la compatibilità della rispettiva attività con le norme applicabili in materia di protezione dei dati.

Pertanto, tornando all'esempio prima citato, l'ufficio istruzione dell'autorità locale sarà soggetto al RGPD e ad eventuali "specificazioni ulteriori" dell'implementazione del RGPD contenute nelle pertinenti disposizioni della legislazione nazionale in materia di protezione dei dati (o nella sezione dedicata alla protezione dei dati della norma che disciplina funzioni e poteri degli uffici istruzione delle autorità locali, che comunque dovrebbe essere conforme alle norme del RGPD).

D'altro canto, l'ufficio di polizia locale sarà soggetto alle disposizioni nazionali adottate in attuazione della DPDPG, nonché a eventuali norme pertinenti contenute nel codice di procedura penale ovvero nella legislazione nazionale in materia di polizia, le quali dovrebbero essere conformi alle norme della DPDPG.

In tal caso, l'ufficio istruzione dell'autorità locale dovrà verificare, con il supporto del proprio RPD ed eventualmente consultando la competente autorità di controllo, se le norme di protezione dati che ne disciplinano l'attività gli consentano di comunicare i dati personali all'ufficio di polizia, e a quali condizioni, o se vietino tale comunicazione.

Viceversa, l'ufficio di polizia locale, prima di rivolgere all'ufficio istruzione la richiesta di fornire i dati, dovrebbe verificare, con l'aiuto del proprio RPD ed eventualmente consultando la competente autorità di controllo, se le norme di protezione dati che ne disciplinano l'attività gli consentano di chiedere o esigere la comunicazione dei dati personali da parte dell'ufficio istruzione locale, e a quali condizioni, ovvero vietino richieste di tal genere.

In molti casi sarà opportuno che i RPD dei due enti esaminino congiuntamente la questione e, ove necessario, rivolgano un'unica richiesta di consultazione all'Autorità di controllo.

Le norme applicabili saranno spesso compatibili e in molti casi l'una rinvierà espressamente all'altra. Per esempio, la legge che disciplina le attività di polizia

potrebbe prevedere quando e a quali condizioni l'ufficio di polizia locale possa chiedere "ad altri soggetti pubblici" di fornire informazioni (generiche e/o con riguardo a minori); e le norme applicabili all'ufficio istruzione potrebbero prevedere che l'ufficio possa (o debba) fornire le informazioni richieste da "un altro soggetto pubblico" (o specificamente dall'autorità di poilzia), purché la richiesta sia lecita. Ciò significa che l'ufficio di polizia dovrebbe rispettare le norme applicabili e le relative condizioni, e l'ufficio istruzione dovrebbe quanto meno chiedere rassicurazioni (documentate) sulla liceità della richiesta avanzata dall'ufficio di polizia e sul rispetto delle condizioni applicabili. A parte ciò, niente osta alla trasmissione dei dati.

Se entrambe le parti in causa, richiedente e richiesta dei dati, sono soggette alle norme Ue recentemente introdotte in materia di protezione dei dati (in particolare, al RGPD, alla DPDPG, e al Regolamento 2018/1725), non dovrebbe esservi alcun problema, in linea generale, per quanto concerne queste trasmissioni di dati – anche se potranno esservi casi particolari meritevoli di analisi più approfondite.

Le questioni in gioco sono di maggiore complessità quando uno dei due soggetti (in particolare, il richiedente) non opera secondo le norme più recenti, ma secondo quelle meno stringenti precedentemente in vigore – che comunque saranno fondate quanto meno sui principi generali in materia di protezione dei dati cui si ispirano tutti gli strumenti giuridici dell'Ue relativi alla protezione dei dati.

La complessità arriva invece a livelli elevatissimi se il soggetto richiedente è del tutto sottratto all'applicazione di norme in materia di protezione dei dati – il che avviene, come abbiamo osservato, nel caso della PESC, delle attività connesse alle missioni Ue per il mantenimento della pace o comunque di natura militare, o della sicurezza nazionale. In un contesto del genere, le norme "adeguate" sono norme chiaramente fondate sui principi generali di protezione dei dati e che riconoscono, quindi, tali principi; che si allontanano dalle norme generali costruite sul fondamento dei principi suddetti solo in quanto ciò sia previsto specificamente da uno strumento giuridico (pubblicamente disponibile, chiaro, preciso) la cui applicazione sia "prevedibile", e soltanto nella misura in cui ciò sia "strettamente necessario" per la specifica finalità e chiaramente "proporzionato" al contesto specifico[208]; e, infine, che prevedono forme di controllo dell'osservanza delle norme speciali in questione a opera di un'autorità indipendente. [209]

Non è questa la sede idonea per un'analisi dettagliata della questione, ma alcune considerazioni di ordine generale si impongono comunque.

La trasmissione di dati personali effettuata da un'autorità pubblica nazionale (o da un'istituzione o organo dell'Ue) soggetta alle norme più recenti in materia di protezione dati (il RGPD, la DPDPG, o il Regolamento 2018/1725) a un'altra autorità o un altro ente dell'Ue che non sia soggetto ad alcuna normativa adeguata in materia di protezione dei dati ha lo stesso potenziale abrasivo in termini di protezione dei dati del trasferimento degli stessi dati effettuato verso un paese privo di norme "adeguate" in materia di

[208] Si tratta dei requisiti dello Stato di diritto delineati dalla giurisprudenza della Corte EDU e applicati anche dalla Corte di giustizia dell'Ue, i quali hanno trovato rispecchiamento nella Carta dei diritti fondamentali dell'Ue e devono essere rispettati da ogni stato democratico in ogni ambito di attività che possa incidere sui diritti e sulle libertà fondamentali della persona.

[209] Come prevede espressamente l'Art. 8, paragrafo 3, della Carta.

protezione dei dati – trasferimento vietato, in linea di principio, salva l'esistenza di "garanzie adeguate" (v. Capo V del RGPD).

Ne consegue che ogni autorità o ente soggetto agli strumenti più recenti adottati dall'Ue in materia di protezione dei dati dovrebbe esercitare particolare cautela nel fornire dati personali che tale ente o autorità tratta nel rispetto degli strumenti suddetti a un'autorità o un ente che non è soggetto ad alcuna norma adeguata in materia. È opportuno verificare attentamente, come sempre con l'aiuto del RPD ed eventualmente previa consultazione della competente autorità di controllo, se lo strumento applicabile a quell'ente o autorità consente la trasmissione in oggetto ovvero la vieta o prevede specifiche condizioni al riguardo; l'ente o l'autorità dovrebbe, dunque, rifiutarsi di trasmettere i dati se tale trasmissione non è consentita in misura sufficientemente inequivocabile dallo strumento giuridico che ne disciplina l'attività.

Non è sufficiente che un soggetto richiedente i dati cui non si applichino norme adeguate in materia di protezione dei dati evidenzi al soggetto richiesto che l'ottenimento (la raccolta) dei dati in questione è consentito dalle norme applicabili al richiedente stesso. Una norma del genere potrà legittimare la raccolta dei dati, ma non legittima la comunicazione ("trasmissione") dei dati stessi da parte del soggetto richiesto in base alle diverse norme in materia di protezione dati che si applicano a quest'ultimo – soprattutto ove tali norme siano fissate in uno degli strumenti recenti prima menzionati relativi alla protezione dei dati ovvero siano adottate sulla base di uno degli strumenti suddetti.

In taluni Stati sono tuttora in vigore disposizioni di legge che conferiscono ad alcune agenzie nazionali, in particolare i servizi di sicurezza, il diritto di esigere informazioni o l'accesso a informazioni, anche personali, in termini estremamente lati; alcune di tali norme sono formulate in modo tale da prevalere su qualsiasi limitazione alla comunicazione di dati personali da parte di altri enti soggetti alla legislazione in materia di protezione dei dati, i quali – secondo quanto previsto da tali norme di latissima applicazione – devono ottemperare alle richieste a prescindere da quanto stabilisce la norma di protezione dati normalmente applicabile alle loro attività. Questa è la situazione riscontrabile anche in alcuni Stati membri dell'Ue.[210]

Con riguardo alle agenzie per la sicurezza nazionale, alcuni Stati membri affermano che le norme che conferiscono a tali agenzie il potere di esigere informazioni (o l'accesso a banche dati) esulano dal campo di applicazione del diritto dell'Ue, e che pertanto anche la trasmissione di dati a tali agenzie prevista dal diritto nazionale è sottratta all'applicazione del diritto Ue e alla competenza delle autorità di protezione dati o della Corte di giustizia dell'Ue.

Tuttavia, si tratta di un'interpretazione erronea del quadro giuridico di riferimento. Anche se la raccolta di dati personali da parte di tali agenzie non ricade nel campo di applicazione del diritto dell'Ue (né nella competenza delle autorità di controllo o della Corte di giustizia dell'Ue), la trasmissione dei dati a tali agenzie da parte di soggetti le cui attività sono disciplinate da strumenti Ue in materia di protezione dei dati ricade pienamente nell'ambito del diritto dell'Ue. I titolari coinvolti e i loro RPD dovrebbero sensibilizzarsi al riguardo e consultare la rispettiva autorità di controllo ogniqualvolta

[210] V. Douwe Korff et al, Boundaries of Law (nota 168, *supra*), Parte 4.

insorgano situazioni così controverse.

1.4.7 La Convenzione ("aggiornata") del Consiglio d'Europa sulla protezione dei dati del 2018

Benché la Convenzione del Consiglio d'Europa del 1981 sia stata (ampiamente) armonizzata con la Direttiva sulla protezione dei dati personali CE del 1995, grazie all'aggiunta di norme sui flussi trasfrontalieri di dati e alla creazione di autorità indipendenti sulla protezione dei dati figuranti nel Protocollo addizionale adottato nel 2001 (come visto al punto 1.3.2, *supra*), si trattava di un testo che, come la Direttiva, nel primo decennio del XXI sec. risultava ormai superato. I lavori di "ammodernamento" della Convenzione cominciarono nel 2011, e la "Convenzione aggiornata" venne adottata il 18 maggio 2018 e aperta alla firma il 10 ottobre 2018.[211] Al momento della stesura, questo testo (dicembre 2018) non è ancora in vigore: l'entrata in vigore sarà possibile o con il consenso unanime di tutte le Parti, o dopo 5 anni dall'apertura alla firma se vi sono almeno 38 stati che hanno espresso il loro consenso a vincolarsi al Protocollo, il quale, naturalmente, avrà valore solo per loro[212]; (art. 37). per quanto riguarda gli altri Stati firmatari della Convenzione del 1981 (e, se di applicazione, del Protocollo aggiuntivo), continueranno ad essere di applicazione la vecchia Convenzione (e il Protocollo).[213]

Lo stesso Consiglio d'Europa ha elaborato un'utile **relazione** delle **novità contenute nella Convenzione aggiornata**:[214]

> Le novità principali[215] della Convenzione aggiornata possono così essere riassunte:
>
> **Obiettivo e scopo della Convenzione (Articolo 1)**

---

211 Si veda:
https://www.coe.int/en/web/data-protection/background-modernisation
Il testo unico della Convenzione aggiornata del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale è disponibile su:
https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf –
Al momento della stesura di questo testo (agosto 2018) il Protocollo aggiuntivo (CETS 223) non era ancora disponibile nella banca dati dei Trattati del Consiglio d'Europa:
https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/search/CETS

212 Nelle more dell'entrata in vigore, le Parti della Convenzione possono comunque dichiarare di voler applicare il Protocollo in via transitoria. In tal caso i principi della Convenzione si applicheranno nei confronti delle altre Parti che hanno fatto una simile dichiarazione.

213 Alla metà di dicembre del 2018 la Convenzione modernizzata era stata sottoscritta da 22 Stati, ma nessuno l'aveva ancora ratificata. Si veda: https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/223/signatures?p_auth=ZmXAeCCF
Lo Special Rapporteur delle Nazioni Unite sul diritto alla privacy ha raccomandato una ratifica globale della Convenzione "aggiornata" fin dal 2018.

214 Tratto da:
https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8
Tutti i dettagli relativi alle modifiche del testo sono disponibili in forma sinottica su:
https://rm.coe.int/cahdata-convention-108-table-e-april2018/16808ac958 (26 pagine)

215 La relazione illustra solo le novità, senza riprendere le norme già fissate nella Convenzione del 1981 e nel Protocollo aggiuntivo del 2001. Per una panoramica completa della Convenzione aggiornata, si consulti la versione consolidata nel sito web del Consiglio d'Europa (nota originale con modifiche).

L'obiettivo della Convenzione risulta charamente enunciato all'Articolo 1 della stessa: garantire ai soggetti interessati all'interno della giurisdizione di uno Stato firmatario (indipendentemente dalla nazionalità o dal luogo di residenza) la protezione dei loro dati personali, quando oggetto di un trattamento, contribuendo al rispetto dei diritti e delle libertà fondamentali dei singoli, in particolare il diritto alla privacy.

Con questa formulazione, la Convenzione sottolinea il fatto che il trattamento dei dati personali possa positivamente consentire l'esercizio effettivo di altri diritti e libertà fondamantali, la cui facilitazione è garantita dal diritto alla protezione dei dati.

Definizioni e ambito di applicazione (Articoli 2 e 3)

Se alcune definizioni, come quelle di dati personali o di soggetto interessato, non sono state modificate,[216] nelle definizioni appaiono alcuni cambiamenti: il concetto di 'file' viene abbandonato. 'Titolare di un file di dati' viene sostituito da 'titolare del trattamento', e vengono aggiunti i termini di 'responsabile del trattamento' e 'destinatario'.

L'ambito di applicazione riguarda sia il trattamento automatizzato che quello non automatizzato dei dati personali (o trattamento manuale, in cui i dati fanno parte di una struttura che rende possibile la ricerca per soggetto interessato secondo criteri prefissati) che rientrino nella giurisdizione dei firmatari della Convenzione. La natura *omnibus* della Convenzione viene mantenuta e l'ambito di applicazione continua, naturalmente, a riguardare sia il trattamento nel settore pubblico che in quello privato (indistintamente), uno dei grandi punti di forza della Convenzione.

Per converso, la Convenzione non è più di applicazione al trattamento dei dati operato da una persona fisica nell'esercizio di attività puramente personali e domestiche.[217]

Inoltre, i firmatari non godono più della possibilità di esentare dall'applicazione della Convenzione determinate tipologie di trattamento dei dati (ad es. per scopi di sicurezza nazionale o di difesa).

Impegni delle parti (Articolo 4)

Ciascuna Parte adotta, nell'ambito del suo diritto interno, le misure necessarie per dare effetto ai principi fondamentali della Convenzione.

Inoltre, i firmatari debbono dimostrare che tali misure sono state attuate, che sono efficaci e accettare che il Comitato della Convenzione verifichi l'adempimento dei requisiti. Questo [*nuovo*] iter di valutazione delle Parti ("meccanismo di follow-up") deve garantire che il livello di protezione fissato dalla Convenzione sia quello che i firmatari possono tutelare.

E' importante rilevare che le organizzazioni internazionali hanno adesso la possibilità di accedere alla Convenzione (Articolo 27), e questo vale anche per l'UE (Articolo 26).

Legittimità del trattamento dei dati e qualità dei dati (Articolo 5)

L'Articolo 5 chiarisce l'applicazione del principio di proporzionalità e sottolinea come debba esseree applicato nell'arco dell'intero trattamento, e in particolare, nel rispetto

---

216 Rileviamo che ampie annotazioni figurano nella Relazione esplicativa alla Convenzione aggiornata (nota aggiunta).

217 Tale "trattamento prettamente personale" venne dapprima escluso dalle norme sulla protezione dei dati nella Direttiva del 1995 per garantire il rispetto del diritto alla vita privata; è stato ripreso, invece, nel RGPD (nota aggiunta).

di metodi e procedure utilizzate nel trattamento. Il concetto viene ulteriormente rinforzato dal principio della minimizzazione dei dati.

Per chiarire in modo inequivoco la base giuridica del trattamento, è stata introdotta una nuova disposizione: il consenso (che per essere valido deve soddisfare determinati criteri) dell'interessato o altre basi giuridiche determinate per legge (contratto, interesse vitale dell'interessato, obblighi giuridici del titolare, ecc.).

Dati sensibili (Articolo 6)

La lista dei dati sensibili è stata ampliata ad includere dati genetici e biometrici (con una certa influenza sull'UE) e dati trattati per le informazioni che possono rivelare sull'appartenenza sindacale o l'origine etnica (queste due categorie sono state aggiunte al divieto già esistente [*in principio*] di trattamento dei dati personali che rivelino le opinioni politiche, le convinzioni religiose o altre convinzioni, nonché i dati a carattere personale relativi alla salute o alla vita sessuale e i dati a carattere personale relativi a condanne penali).

Sicurezza dei dati (Articolo 7)

Per quanto riguarda la sicurezza dei dati, viene introdotto l'obbligo tempestivo di notifica di ogni violazione della sicurezza. L'obbligo è limitato a quei casi che possono seriamente pregiudicare i diritti e le libertà fondamentali degli interessati; le violazioni devono essere notificate almeno alle autorità di controllo.

Trasparenza del trattamento (Articolo 8)

I titolari del trattamento hanno l'obbligo di garantire la trasparenza del trattamento dei dati e, a tale scopo, devono fornire tutta una serie di informazioni, in particolare quelle relative alla loro identità, luogo abituale di residenza/sede, basi legali, finalità del trattamento, destinatari dei dati e categorie dei dati personali trattati. Devono inoltre fornire ogni informazione necessaria a garantire un trattamento equo e trasparente. Il titolare del trattamento è esentato dal fornire tali informazioni qualora esista in materia un'espressa prescrizione di legge o possa provare che tale compito si riveli impossibile o impegni risorse sproporzionate.

Diritti del soggetto interessato (Articolo 9)

Nell'era digitale sono stati garantiti agli interessati nuovi diritti che permettono loro un controllo maggiore sui dati che li riguardano.

La Convenzione aggiornata amplia la lista delle informazioni da trasmettere agli interessati nell'esercizio del loro diritto di accesso. Inoltre, gli interessati possono venire a conoscenza del motivo che determina il trattamento dei dati e dei risultati che si applicheranno loro. Si tratta di un nuovo diritto che è particolarmente importante per la profilazione dei singoli.[218]

Questa novità va vista in congiunto con un'altra norma nuova, il diritto, per l'interessato, di non essere soggetto ad una decisione presa unicamente sulla base di un trattamento automatizzato, senza che il parere dell'interessato sia stato preso in considerazione.

[218] Sull'argomento si veda la Raccomandazione (2010) 13 sulla protezione delle persone fisiche con riguardo al trattamento automatizzato dei dati personali nel contesto di attività di profilazione e il Memorandum esplicativo a questo testo (nota originale).

Gli interessati possono opporsi in ogni momento al trattamento dei loro dati personali, ad eccezione che il titolare dimostri l'esistenza di motivi preminenti e legittimi per il trattamento, motivi che siano anteponibili a interessi, diritti e libertà fondamentali.

Obblighi supplementari (Articolo 10)

La Convenzione aggiornata impone obblighi più stringenti sui titolari del trattamento o su coloro che operano a loro nome e titolo.

La responsabilizzazione diventa parte integrante degli strumenti di protezione, con l'obbligo, per i titolari del trattamento, di dimostrare l'adempienza delle disposizioni sulla protezione dei dati.

I titolari del trattamento devono adottare misure appropriate, anche quando il trattamento è esternalizzato, per garantire il diritto alla protezione dei dati (tutela della privacy fin dalla progettazione ["privacy by design"], esame del possibile impatto del trattamento dei dati cui si intende procedere sui diritti e le libertà fondamentali dell'interessato ("valutazione d'impatto sulla privacy") e impostazioni predefinite a tutela della vita privata ("privacy by default").

Eccezioni e limitazioni (Articolo 11)

I diritti sanciti dalla Convenzione non sono assoluti e possono subire limitazioni per legge o qualora le limitazioni costituiscano una misura necessaria in una società democratica sulla base di motivi specifici e molto circoscritti, fra i quali figurano anche "essenziali obiettivi di interesse pubblico", nonché un riferimento al diritto di libertà di espressione.

La lista delle norme della Convenzione che possono subire limitazioni è stata notevolmente ampliata (si vedano i riferimenti all'Articolo 7.1, in materia di sicurezza, e 8.1, in materia di trasparenza, all'Articolo 11.1); un nuovo paragrafo di questo articolo tratta specificamente delle attività di trattamento a scopo di sicurezza nazionale e di difesa, per le quali i poteri di "monitoraggio" del Comitato e alcuni compiti delle Autorità di supervisione possono essere limitati. Molto chiaro è il dettato della disposizione per cui le attività di trattamento a fini di sicurezza nazionale e di difesa sono subordinate ad una vigilanza e ad un controllo efficaci e indipendenti.

Ancora una volta è importante ricordare che, contrariamente alle precedenti disposizioni della Convenzione 108, i firmatari della Convenzione aggiornata non hanno più facoltà di escludere, dal campo di applicazione della Convenzione, determinati tipi di trattamento.

Flussi transfrontalieri di dati personali (Articolo 14)[219]

Questa disposizione mira a facilitare, quando di applicazione, il libero flusso delle informazioni senza limiti di frontiere garantendo, nel contempo, una tutela appropriata degli interessati in materia di protezione dei dati personali.

In assenza di norme di protezione armonizzate condivise dagli Stati che appartengono ad organizzazioni regionali internazionali e che disciplinano flussi informativi (si veda, ad es., il quadro di riferimento sulla protezione dei dati dell'Unione Europea), i flussi di dati fra le Parti devono essere trasmessi liberamente.

Per quel che riguarda il flusso transfrontaliero di dati verso un destinatario che non è soggetto alla giurisdizione di una Parte, deve essere garantito un appropriato livello di protezione nello Stato o nell'organizzazione destinataria. Poiché questa presunzione

219 In tal senso, la Convenzione aggiornata si basa sul Protocollo aggiuntivo e sulla normativa UE.

non può essere garantita, visto che il destinatario non è una Parte, la Convenzione fissa due misure per garantire che il livello di protezione dei dati sia quello appropriato: o per legge, o tramite garanzie armonizzate, ad hoc o concordate, che abbiano carattere vincolante, applicabile (parliamo, in particolare, delle clausole contrattuali o delle norme vincolanti d'impresa), nonché debitamente attuabile.

Autorità di controllo (Articolo 15)

Basandosi sull'Articolo 1 del Protocollo aggiuntivo, la Convenzione aggiornata completa il catalogo dei poteri delle Autorità di controllo, stabilendo che, oltre ai poteri di intervento, di indagine, di azione in giudizio o denuncia alle autorità giudiziarie delle violazioni delle norme della protezione dei dati, le Autorità abbiano anche il dovere di far nascere una maggiore consapevolezza, fornire informazioni ed educare tutti gli attori coinvolti (soggetti interessati, titolari e responsabili del trattamento, ecc.). Alle Autorità viene anche garantita la possibilità di prendere decisioni e imporre sanzioni. Si ricorda, inoltre che, le Autorità di controllo devono essere indipendenti nell'esercizio di questi poteri e di questi compiti.

Forme di cooperazione (Articolo 17)

La Convenzione aggiornata tratta anche del problema della cooperazione (e mutua assistenza) fra Autorità di controllo.

Le Autorità di controllo hanno il dovere di coordinare le loro inchieste, sviluppare azioni comuni e fornirsi a vicenda informazioni e documentazione sulle rispettive prassi giuridiche e amministrative in materia di protezione dei dati.

Le informazioni oggetto di scambio fra le Autorità di controllo comprendono anche i dati personali, ma solo nel caso in cui questi siano essenziali alla cooperazione o qualora l'interessato abbia fornito il suo consenso specifico, libero e informato.

La Convenzione, infine, prevede un'istanza di potenziamento della cooperazione; le Autorità di controllo delle Parti hanno l'obbligo di creare una rete per organizzare la mutua cooperazione e adempiere ai propri doveri ai sensi della Convenzione.

Il Comitato della Convenzione (Articoli 22, 23 e 24)

Il Comitato della Convenzione ha un ruolo fondamentale nell'interpretare la Convenzione, incoraggiare lo scambio di informazioni fra le Parti e sviluppare le norme di protezione dei dati.

La Convenzione aggiornata ha rafforzato sia il ruolo che i poteri di questo Comitato, non è più limitato ad un ruolo "consultativo", ma investito di poteri di valutazione e di monitoraggio. [*Oltre ad elaborare*] pareri sul livello di protezione dei dati garantito da uno Stato, *[come accadeva in precedenza], il Comitato è ora chiamato a pronunciarsi sulle organizzazioni internazionali* prima dell'adesione alla Convenzione. Inoltre, è [*oggi*] chiamato a valutare la conformità del diritto nazionale della Parte interessata e a determinare l'efficacia delle misure intraprese (esistenza di Autorità di controllo, responsabilità precipue, esistenza di efficaci mezzi giurisdizionali).

Inoltre è in grado di valutare se le norme che disciplinano il trasferimento dei dati garantiscano in modo sufficiente un livello appropriato di protezione dei dati.

Non è qui il caso di analizzare nel dettaglio tutte queste novità; basti notare che tali norme **avvicinano il nuovo regime della Convenzione "aggiornata" al nuovo regime stabilito per l'UE ai sensi del RGPD**. Questo significa che, quando l'UE sarà chiamata a valutare l'"adeguatezza" del regime di protezione dei dati di un paese terzo (come vedremo nella

Seconda Parte, sezione 2.1), il fatto che tale paese sia una Parte della Convenzione aggiornata costituirà un elemento molto importante di valutazione.

Per quanto riguarda il **campo di applicazione**, la Convenzione aggiornata supera il RGPD, come emerge chiaramente sia dal testo della Convenzione stessa che dalla disamina fatta, in quanto i firmatari della Convenzione aggiornata non potranno più escludere dai loro obblighi alcun tipo di trattamento – come quelli derivanti dalla ***sicurezza nazionale*** e dalla ***difesa***, che vengono a ritrovarsi al di fuori del campo di applicazione degli strumenti sulla protezione dei dati dell'UE.[220]

Se, come in altri casi, la Convenzione aggiornata – o, per essere più precisi, la legislazione nazionale dei firmatari della Convenzione aggiornata che attua tale Convenzione – sarà pienamente in linea con il RGPD – o, per essere più precisi, con il RGPD nella sua intepretazione e applicazione futura da parte del nuovo Comitato Europeo per la protezione dei dati dell'UE, delle Autorità sulla protezione dei dati degli Stati membri dell'UE, della Commissione Europea e della CGUE – è questione che sarà necessario verificare in futuro.

Per fare un esempio, le nuove norme sui flussi transfrontalieri di dati nella Convenzione aggiornata consentono trasferimenti verso paesi terzi che garantiscano un "***appropriato***" livello di protezione (Art. 14) – che può apparentemente assimilarsi alla disposizione di un "***adeguato***" livello di protezione previsto dal RGPD (come figurava anche nella Direttiva sulla protezione dei dati del 1995) – ma resta da capire se o in che modo il nuovo Comitato della Convenzione segua la posizione della CGUE nel ritenere che il termine "appropriato" debba essere interpretato nel senso che il paese terzo in questione debba garantire una protezione "***sostanzialmente equivalente***" (come stabilito dalla CGUE nell'interpretazione del termine "adeguato").[221]

Sotto altri aspetti, invece, come il **consenso dei minori**, la Convenzione aggiornata non è così dettagliata e specifica come il RGPD.

Tralasciando, comunque, questi problemi, emerge chiaramente che il Consiglio d'Europa e l'Unione Europea hanno aperto la strada nel fissare le "regole d'oro" a livello globale in materia di protezione dei dati, sia quelle applicabili agli Stati, che quelle riguardanti i flussi transnazionali di dati.

Notiamo, quale ultimo punto, che la Convenzione aggiornata, a differenza del testo che la precedeva, è aperta alla firma delle organizzazioni internazionali – e che l'UE ha facoltà di aderirvi formalmente.

- o – O – o -

---

220 Si veda la sezione 1.3.1, *supra*, alla sezione "*Natura e limiti delle Direttive CE*", per quanto riguarda questa limitazione in relazione alle Direttive CE di protezione dei dati del 1995 e del 2002, nonché la Seconda Parte, sezione 2.1, *infra*, per quanto riguarda il RGPD. In materia di trattamento per finalità riguardanti le forze dell'ordine (ecc.) e trattamento effettuato dalle stesse istituzioni dell'UE, ricordiamo che l'UE dispone di tutta una serie di norme in vigore, che sono sostanzialmente conformi alle disposizioni del RGPD (e quindi a quelle della Convenzione aggiornata). Per quanto riguarda le istituzioni dell'UE, tali norme saranno conformi dopo l'armonizzazione con il RGPD.

221 CGUE, Sentenza *Schrems* (nota 73, *supra*), paragrafo 73.

PARTE II

Il Regolamento Generale sulla Protezione dei Dati - RGPD

2.1 Introduzione

Come già menzionato al punto 1.4.1, *supra*, il Regolamento generale sulla protezione dei dati (RGPD o "il Regolamento") è stato adottato, in parte, per il fatto che la Direttiva sulla protezione dei dati personali del 1995 non ha portato ad un livello sufficiente di armonizzazione fra le legislazioni degli Stati membri, in parte, come risposta alla massiccia espansione nel trattamento dei dati personali dall'introduzione della Direttiva sulla protezione dei dati personali del 1995 e, in parte, come risposta alla giurisprudenza della CGUE. Resta da vedere se questo strumento si rivelerà sufficiente per rispondere appieno agli sviluppi di tecnologie sempre più intrusive, come i Big Data, l'Internet degli oggetti, processi decisionali effettuati con strumenti algoritmici e utilizzo dell'intelligenza artificiale.

Il Regolamento si basa sulla Direttiva sulla protezione dei dati personali del 1995 ma ne amplia significativamente la portata e, al contempo, introduce disposizioni considerevolmente più robuste in materia di protezione dei dati dell'UE. Il Regolamento garantisce una *maggiore armonizzazione, maggiori e più forti diritti ai soggetti interessati, cooperazione rafforzata fra le Autorità di protezione dei dati, maggiori poteri di applicazione* – e molto altro.

L'allegato 1 a questo Manuale fornisce un *Indice dei capitoli, delle sezioni e degli articoli del RGPD,* per una più rapida lettura. L'Allegato 2 fornisce il testo integrale del Regolamento come pubblicato nella Gazzetta Ufficiale dell'UE, compresi i considerando.

La sezione 2.2 illustra lo status giuridico e l'approccio procedurale del RGPD e discute nel dettaglio le implicazioni delle molte clausole contenute nel testo che lasciano margini per un'ulteriore regolamentazione a livello nazionale (quindi minando in parte l'obiettivo di una maggiore armonizzazione).

La sezione 2.3 offre uno spaccato del RGPD capitolo per capitolo, sezione per sezione e articolo per articolo. Al momento opportuno verrà offerto un breve commento sulle disposizioni analizzate, con un focus particolare sulle norme del Regolamento che, rispetto alla Direttiva sulla protezione dei dati del 1995, risultano essere una novità, presentano importanti ampliamenti rispetto al passato, chiariscono o regolamentano ulteriormente problematiche che non erano state normate del tutto o lo erano state in modo più dettagliato.

Passeremo poi a trattare due elementi caratterizzanti per i RPD: il nuovo principio di "responsabilizzazione" (obbligo di dimostrazione dell'ottemperanza), alla sezione 2.4, e le norme che regolamentano nomina, requisiti, condizioni, compiti, ecc. dei RPD (sezione 2.5).

2.2 Status giuridico e approccio procedurale del RGPD: applicabilità diretta e "clausole di specificazione"

Un Regolamento …

Il RGPD è un **regolamento** – cioè uno strumento legislativo del Diritto comunitario di ***applicazione diretta*** negli ordinamenti giuridici degli Stati membri dell'UE (e anche degli Stati non UE/SEE) e che non necessita di "recepimento" nel diritto nazionale, come è il caso delle direttive, come la Direttiva sulla protezione dei dati personali del 1995.

Il legislatore europeo ha scelto questo strumento proprio perché il recepimento della Direttiva del 1995 era stato disomogeneo: il dettato era stato recepito in modo diverso nei differenti Stati membri determinando una mancanza di armonizzazione.[222]

Inoltre, il testo era stato recepito in maniera lacunosa in almeno una serie di Stati, fra cui il Regno Unito.[223]

In teoria, un regolamento, avendo un'applicazione diretta, dovrebbe generare una **piena armonizzazione** della giurisprudenza del settore cui si riferisce. Nel caso del RGPD, questa tendenza è stata rafforzata da norme più cogenti per la **condivisione delle informazioni e la cooperazione** fra regolatori (le Autorità nazionali di controllo - o Autorità di protezione dei dati, DPA) e da uno speciale **meccanismo di "coerenza"**, come vedremo in questa parte.

Come avremo modo di rilevare nella prossima sottorubrica, comunque, il RGPD lascia sul tappeto molti problemi aperti che richiederanno di essere ulteriormente normati nei diritti nazionali degli Stati membri conformemente al rispettivo sistema giuridico o istituzionale. Questa necessità potrebbe, almeno in alcuni settori, mettere in pericolo il fine di una piena armonizzazione, sebbene, come rileveremo alle sezioni "*Requisiti delle "clausole di specificazione*" e "*Cooperazione e coerenza*", esistono comunque sia dei limiti alla libertà degli Stati membri sotto questo profilo che dei nuovi strumenti di supervisione, a livello UE, per l'esercizio di queste "flessibilità" (almeno in teoria).

… ma con "clausole di specificazione"[224]

Sebbene il Regolamento miri ad una maggiore armonizzazione, contiene molte norme che rimandano alla legislazione degli Stati membri (le cosidette "disposizioni flessibili", denominate dalla Commissione "clausole di specificazione"), soprattutto in relazione al settore pubblico, ma anche in relazione ad obblighi imposti dal diritto nazionale ad aziende sottoposte alla giurisdizione di uno Stato membro (ad es., le leggi che regolamentano la disoccupazione o quelle di ambito giudiziario) e anche per quanto riguarda la struttura delle autorità di controllo.

Tipologie di disposizioni "flessibili"

L'Autorità italiana della protezione dei dati, il *Garante della Privacy*, ha identificato quattro diversi tipi di clausole (benché alcune delle quali coincidano in parte) che lasciano spazio ad un'ulteriore regolamentazione nazionale da parte degli Stati membri:[225]

---

[222] Questa conclusione era già stata raggiunta dallo studio di Douwe Korff per l'Università dell'Essex commissionato dall'UE: Report on an EU study on the implementation of the [1995] data protection directive, 2002, disponibile su:
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667
Ci sono voluti altri 10 anni all'UE per risolvere il problema con la proposta di un Regolamento.

[223] Secondo la Commissione Europea, nel 2011, circa un terzo dei 34 articoli della Direttiva non erano ancora stati recepiti correttamente dal Regno Unito, si veda:
http://amberhawk.typepad.com/amberhawk/2011/02/european-commission-explains-why-uks-data-protection-act-is-deficient.html
Anche se la Commissione ha minacciato l'adozione di misure coercitive, tali misure non sono mai state adottate e tali carenze non hanno mai trovato un pieno o appropriato rimedio.

[224] Si veda la sotto-sezione, *supra*, dedicata al "Rapporto fra direttiva e-privacy e RGPD".

[225] Antonio Caselli, presentazione alla prima sessione di formazione "T4DATA", giugno 2018, su "*RGPD e normativa nazionale*". Le linee principali della presentazione sono riassunte e approfondite in alcuni dettagli all'Allegato 4 al Manuale (Secondo Volume) che contiene anche ulteriori esempi.

- **Norme specifiche ulteriori**

  Sono norme per le quali uno Stato membro può mantenere o introdurre "*disposizioni più specifiche al fine di adeguare l'applicazione*" delle norme giuridiche del Regolamento (possono essere usate espressioni con dettati differenti).

  Esempi:

  Gli Stati membri possono specificare quali operazioni di trattamento richiedano un'***autorizzazione previa***, oppure disciplinare l'utilizzo dei ***numeri di identificazione nazionale***, o il trattamento dei ***dati personali dei dipendenti***.

  Gli Stati membri possono "*mantenere o introdurre* ***disposizioni ulteriori, comprese limitazioni****, in materia di trattamento di* ***dati genetici, biometrici o relativi alla salute***", ben oltre le condizioni e le limitazioni imposte dallo stesso RGPD all'Articolo 9(1) – (3) (l'articolo che si occupa del trattamento di "categorie particolari di dati personali", abitualmente denominati "dati sensibili") (Art. 9(4)). Tali disposizioni possono, ad es., stabilire che, nel trattamento di **dati genetici**, ***l'autorizzazione previa*** sia sempre obbligatoria.

- **Opzioni e scelte**

  In alcuni casi, il RGPD dà facoltà agli Stati membri, attraverso la normativa nazionale, di **scegliere** fra alcune possibilità specificamente offerte dal regolamento, oppure di estendere ad altri casi un obbligo o un divieto che, ai sensi del RGPD, sia di applicazione solamente a certi casi.

  Per esempio, il RGPD sancisce che il trattamento è lecito ove un minore abbia almeno 16 anni, ma gli Stati membri possono consentire a ***minori*** di 13, 14 o 15 anni di ***prestare il consenso a certi servizi di informazione***; oppure, gli Stati membri possono richiedere **la nomina di un RPD** quando il RGPD non lo preveda.

- **Limitazioni e deroghe**

  A certe **condizioni**, formulate in modo ampio (e di cui parleremo fra poco alla rubrica "*Requisiti delle 'clausole di specificazione'* e "*Problemi relativi alle 'clausole di specificazione' "*), l'Articolo 23 del RGPD impone **limitazioni ben definite** su quasi tutti i diritti dell'interessato in relazione all'ampia definizione degli **obiettivi fondamentali di interesse pubblico**: ***sicurezza nazionale, difesa, pubblica sicurezza, il perseguimento di reati e l'indipendenza dei procedimenti giudiziari*** – ma anche la ***salvaguardia degli interessi economici o finanziari dello Stato***, la salvaguardia dell'***etica professionale***, ogni tipo di "***controllo, ispezione e regolamentazione*** connessa, anche occasionalmente, all'esercizio di pubblici poteri" in ciascuno dei fondamentali intressi tutelati, "la ***tutela dell'interessato o dei diritti e delle libertà altrui***" e l'***esecuzione delle azioni civili***.

  Gli articoli 85, 86 e 89 del RGPD contengono disposizioni che, da un lato, permettono (e, in alcuni casi, richiedono) **deroghe** per determinate norme del RGPD allo scopo di proteggere la **libertà di espressione**, permettere la **libertà di informazione** (accesso a documenti e informazioni nelle mani delle autorità pubbliche) e le attività di **archiviazione**, facilitare (a vantaggio pubblico) la **ricerca**, mentre, dall'altro, impongono determinate **condizioni** a tali deroghe (come vedremo alla sezione

"*Requisiti delle 'clausole di specificazione'* e "*Problemi relativi alle 'clausole di specificazione"*, *infra*).

Nota: alcune di queste norme speciali sono finalizzate a tutelare gli interessi "altrui", mentre in alcuni casi il concetto di altrui può essere interpretato come 'di interesse pubblico o generale' e alcuni concetti, come quello di libertà dell'informazione, possono coprire entrambi. Si tratta di ambiti in cui le normative non sono state sinora armonizzate, benché, in alcuni Stati membri dell'UE, sia la supervisione della protezione dei dati che quella della libertà di espressione siano state affidate alle stesse autorità. Dato che tali problematiche hanno sempre più una valenza transnazionale – pensiamo alle richieste transfrontaliere di accesso a dati pubblici, alla libertà d'espressione in opposizione alla protezione dei dati e alla privacy nelle pubblicazioni online, alla ricerca medica transnazionale – è probabile che il Comitato Europeo per la protezione dei dati (EDPB) sarà chiamato ad esprimersi su tali questioni, in particolare quelle relative alle attività transnazionali. Anche la Commissione ha il potere di proporre nuove iniziative in questi ambiti.

- **Obblighi di regolamentazione**

  Per quanto riguarda altri elementi – in particolare, la creazione di organismi indipendenti di controllo (le autorità di protezione dei dati o DPA), e la creazione di schemi di certificazione – il RGPD **obbliga** gli Stati membri ad adottare norme e disposizioni dettagliate per il recepimento, nella legislazione nazionale, di quanto stabilito in materia di DPA. Si tratta, in gran parte, di normative molto tecniche (che richiedono comunque la conformità ad importanti requisiti come, ad es., quello dell'indipendenza e la disponibilità di risorse sufficienti).

Requisiti delle "clausole di specificazione"

Sotto vari profili, compresi quelli cui si fa riferimento alla sezione "*specificazioni ulteriori*" e "*scelte ed opzioni*", *supra*, ma soprattutto quelli analizzati alla sezione "*limitazioni e deroghe*", il RGPD **impone** agli Stati membri di adottare ***norme giuridiche*** per trattare specifiche materie che ***soddisfino alcuni requisiti democratici o relativi ai diritti umani.***

Anche altre norme (che non figurano in queste sezioni) **implicano una necessità di regolamentazione**, nel senso che impongono agli Stati membri di adottare "***garanzie adeguate***", "***opportune salvaguardie***" o "***misure adeguate***". Dal momento che il RGPD non chiarisce di quali misure o salvaguardie si tratti, gli Stati membri dovranno chiarire tali concetti nelle rispettive legislazioni nazionali – che, ancora una volta, dovranno rispettare determinate **norme** democratiche e proprio di uno stato di diritto.

È importante rilevare che, in questo, gli Stati membri **non godono di un potere discrezionale esclusivo e illimitato** – come si evince chiaramente dal fatto che certe misure e salvaguardie debbano essere "adeguate" o "opportune". In altri casi, invece, alcune regole e condizioni di applicazione generale relative al rispetto dei requisiti dello stato di dirittosono chiaramente esplicitate nel RGPD – anche se, di fatto, trovano applicazione in ogni ambito normativo.

Quindi, il RGPD afferma chiaramente che le deroghe, in principio radicali e di cui all'Articolo 23 (riassunte alla rubrica "*Limitazioni e deroghe*")[226] debbano essere fissate per **legge** (una "***misura legislativa***") e che tale legge "***rispetti [] l'essenza dei diritti e delle libertà***

[226] Si veda la nota 49, *supra*.

fondamentali *e costituisca una misura* ***necessaria e proporzionata*** *in una società democratica*" per la salvaguardia dei suoi interessi. Si tratta di norme che sono un riflesso diretto di quelle che devono essere rispettate dalle limitazioni imposte ai diritti fondamentali tutelati dalla Convenzione Europea dei diritti dell'uomo (CEDU) e dalla Carta dei diritti fondamentali dell'UE (CDF). Possiamo citare quest'ultimo testo:

> "Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e **rispettare il contenuto essenziale** di detti diritti e libertà. Nel rispetto del principio di **proporzionalità**, possono essere apportate limitazioni solo laddove siano **necessarie** e **rispondano effettivamente a finalità di interesse generale** riconosciute dall'Unione o **all'esigenza di proteggere i diritti e le libertà altrui"**.
>
> (Art. 52(1), grassetti aggiunti)
>
> **Poichè la legislazione nazionale di un qualunque Stato membro, che limiti o circoscriva i diritti di una qualsivoglia persona interessata ai sensi di una delle "clausole di specificazione" del RGPD, deve essere considerata un'intrinseca limitazione al diritto alla protezione dei dati come garantito dalla Carta dei diritti fondamentali dell'UE (Articolo 8), i principi di cui sopra devono obbligatoriamente essere rispettati.**

Più nel dettaglio, ai sensi della Convenzione europea, della Carta e anche del RGPD, le disposizioni di legge devono rispondere ad alcuni, cruciali, **requisiti di "qualità"**: le norme giuridiche devono essere "**compatibili con le norme del diritto**" (il che significa, in particolare, che non possono avere un carattere ***discriminatorio*** o ***arbitrario***, devono poter essere ***impugnabili*** e ***oggetto di ricorso efficace***) e, più in particolare, **accessibili** (cioè ***pubblicate e diffuse***) nonché sufficientemente **chiare** e **precise** da essere "***prevedibili***" nella loro applicazione.[227]

Il riferimento al "rispetto del contenuto **essenziale**" dei diritti e delle libertà in oggetto, deve essere inteso come la **proibizione per ogni norma di diritto di ledere a tal punto un diritto da inficiarne la validità**. Per esempio, la Corte di Giustizia dell'UE ha stabilito in particolare che:[228]

> "si deve ritenere che una normativa che consente alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche pregiudichi il contenuto essenziale del diritto fondamentale al rispetto della vita privata, come garantito dall'articolo 7 della Carta"…

Per queste ragioni, le deroghe degli Stati membri a quanto disposto dall'Articolo 23 del RGPD, incluse quelle alle norme sulla protezione dei dati a fini di salvaguardia nazionale e di difesa, non possono mai rivestire, sia a livello di garanzie che di ammissibilità, un carattere inaccettabile ed eccessivo rispetto alle norme giuridiche fondamentali.

---

227 Si veda: Harris, O'Boyle & Warbrick, Law of the European Convention on Human Rights, 2^ ed., 2009, Capitolo 8, sezione 3, *Limitazioni*. Per una panoramica delle norme fondamentali della CEDU, si veda: Douwe Korff, The standard approach under articles 8 – 11 ECHR and article 2 ECHR (dispense didattiche), su: https://www.pravo.unizg.hr/_download/repository/KORFF_-_STANDARD_APPROACH_ARTS_8-11_ART2.pdf Si veda in particolare, in tale dispense, il testo al punto 3 (Diritto) e 5 (Necessario e proporzionato).

228 *Maximillian Schrems contro Commissario alla protezione dei dati*, Sentenza della CGUE nella Causa C-362/14, 6 dicembre 2015, paragrafo 94.

Nello specifico, qualunque deroga all'Articolo 23, e, a maggior ragione, qualsiasi allontanamento dalle norme del RGPD in "clausole di specificazione" deve superare il test del "**necessario e proporzionato in una società democratica**". Questo significa che ogni deroga alle norme di diritto o ogni limitazione dei diritti fondamentali della persona che si basi su "clausole di specificazione", deve perseguire il fine autentico dello "***scopo legittimo***"/"***importante obiettivo di interesse pubblico***", rispondere a "***esigenze sociali inderogabili***" ed essere "***ragionevolmente proporzionata***" al fine perseguito. Nel giudicare che cosa sia effettivamente necessario in tal senso, gli Stati dispongono di un certo "***margine di valutazione***"[229] – sempre, però, limitato dal fatto che la misura (deroga o limitazione) sia necessaria "***in una società democratica***".

In senso lato, se vi sono **chiari orientamenti** su una questione specifica – come quelli delineatisi ai sensi della Direttiva sulla protezione dei dati del 1995 grazie al Gruppo di lavoro Articolo 29 e al GEPD, e ora ai sensi del RGPD grazie al lavoro del Comitato europeo per la protezione dei dati (che include il GEPD) – e/o se c'è un'**ampia convergenza di vedute** fra gli Stati membri (o le DPA degli Stati membri), allora un allontanamento da tale consenso o da tali orientamenti da parte di uno Stato membro sta probabilmente ad indicare che le misure divergenti (deroghe o limitazioni che vanno oltre ciò che è ritenuto necessario o proporzionato in altri Stati membri) non sono "necessarie" o "proporzionate" "in una società democratica".

Comunque, come vedremo nella prossima sezione, queste criticità non possono essere risolte con "meccanismi di cooperazione e di coerenza operativa" (di cui parleremo dopo, trattandoli separatamente).

Problemi relativi alle "clausole di specificazione"

Ci siamo lungamente soffermati sulle "clausole di specificazione" perchè generano almeno due tipi di problemi ad una corretta ed efficace applicazione del RGPD.

Primo: "clausole di specificazione", per la loro intrinseca natura, daranno vita, **nei diversi Stati membri**, a disposizioni **diverse (più o meno dettagliate) su problemi identici, che saranno un riflesso delle peculiarità nazionali**. Questo non crea grandi problemi in relazione, ad esempio, al trattamento dati che si svolga interamente in uno Stato membro e riguardi solo persone interessate in quello Stato membro. Abbiamo visto però, come già sottolineato, che nel XXI sec., sempre più attività statali hanno ripercussioni internazionali e implicano operazioni di trattamento dei dati personali a carattere transfrontaliero anche nel settore pubblico, e questo non solo in relazione alle attività delle forze dell'ordine o di frontiera. Questo si verifica soprattutto nel caso dell'UE, per le "quattro libertà" che sono alla base del progetto europeo: la libera circolazione di merci, servizi, capitali e persone.

---

229 La dottrina del "margine di valutazione", profondamente radicata nella giurisprudenza della Corte Europea dei diritti dell'uomo, è meno chiaramente espressa nella CGUE, che parla più volentieri di "discrezionalità" o "margine di discrezionalità" accordato agli Stati membri in determinati casi. Per le finalità di questo testo, possiamo dire che la dottrina si riflette sia nella giurisprudenza della Corte di Strasburgo che in quella della Corte di Lussemburgo, anche se a volta in misura diversa e a seconda del contesto. Si veda: Francisco Javier Mena Parras, From Strasbourg to Luxembourg? Transposing the margin of appreciation concept into EU law, Bruxelles, 2008, disponibile su: http://www.philodroit.be/IMG/pdf/fm_transposing_the_margin_of_appreciation_concept_into_eu_law_-_2015-7.pdf

Nello scambio di merci e servizi (offerti ed acquistati) tra le frontiere interne o esterne dell'UE, i dati personali sono il corollario necessario ed essenziale di ogni transazione. Il movimento delle persone implica quello dei loro dati: dati fiscali, pensionistici, di previdenza sociale, medici, anagrafici come matrimoni, figli, divorzi, decessi e residenza. Qualsiasi pagamento (fra privati, fra singoli e organismi privati, fra singoli e agenzie dello stato che possono avere natura fiscale, pensionistica o anagrafica), genera un flusso sia di dati finanziari che di altra natura. *A fortiori* questo accade allorquando il trattamento, o parte di esso, avviene online.

Qualora, in tali circostanze, esistano disposizioni diverse nei differenti Stati membri sul trattamento dei dati in questione, tale situazione è suscettibile di generare potenziali (e potenzialmente gravi) **questioni giuridiche** che dovranno essere risolte caso per caso (e ciò spesso non sarà semplice). Gli esempi che seguono possono ben illustrare la situazione in caso di deroghe e limiti che potrebbero figurare nelle "clausole di specificazione" di cui parlavamo prima:

Esempi

- Se uno Stato membro A impone restrizioni all'utilizzo del numero di identificazione nazionale che un altro Stato membro B non applica, queste restrizioni sono applicabili ad un destinatario (anche pubblico) dello Stato B al quale il numero sia stato trasferito?
- Se uno Stato membro A impone "ulteriori condizioni" o "limitazioni" aggiuntive al trattamento di tutti o alcuni tipi di dati sensibili (ad es., all'uso di dati biometrici o genetici) che un altro Stato membro B non impone, queste condizioni o limitazioni sono di applicazione ad un destinatario (anche pubblico) dello Stato B, qualora i dati siano stati trasferiti a questo destinatario?
- Se uno Stato membro A fissa l'età del consenso all'utilizzo dei servizi di informazione, diciamo a 14 anni e un altro Stato membro B applica l'età proposta dal RGPD (16 anni), può un fornitore di servizi di informazione dello Stato A offrire servizi al ragazzo di 14 anni che si trova nello Stato B sulla base del suo consenso? Il fornitore dovrebbe decidere sulla base dell'indirizzo IP del ragazzo (anche se può essere facilmente "alterato" con l'utilizzo di VPN, persino da un quattordicenne)?
- Se uno Stato membro A chiede la previa autorizzazione alla DPA per il trattamento di dati attinenti al sistema previdenziale e di salute pubblica, e un secondo Stato membro B non lo fa, può un'autorità pubblica dello Stato B trattare dati personali di questa natura appartenenti a soggetti dello Stato A senza previa autorizzazione – come potrebbe essere il caso per i figli di migranti che lasciano i congiunti ed altri figli nel paese di origine per lavorare in un altro Stato membro e a cui vengono versati gli assegni familiari ed altre indennità al coniuge rimasto nel paese di origine? (NB: nel contesto della previa autorizzazione, la DPA di riferimento potrebbe probabilmente richiedere o imporre determinate salvaguardie o restrizioni. Le autorità dello Stato B dovrebbero rispettarle? Ne sarebbero a conoscenza?)

I problemi che abbiamo sollevato sono seriamente aggravati **dall'assenza, nel RGPD, di una norma di "diritto applicabile"** in linea con quanto figurava nella Direttiva sulla protezione dei dati del 1995 (anche se questa disposizione, Articolo 4, sollevava vari interrogativi in rapporto

alle diverse versioni linguistiche e in termini di effettività.[230] E' possible che tale norma sia stata esclusa dal RGPD in quanto, come regolamento, il testo sarebbe stato applicato in maniera totalmente armonizzata – ma, come abbiamo rilevato poc'anzi, nelle (molte) fattispecie che rientrano nelle "clausole di specificazione" (e che dovranno essere affrontate a livello nazionale con specifiche normative) questo non è chiaramente avvenuto.

Il secondo problema è inerente alla **conformità ai requisiti di legge**, trattati nella precedente sottorubrica. Il fatto che certe normative in vigore in certi Stati membri possano limitare determinati diritti o allentare certe disposizioni è destinato a sollevare quesiti di conformità riguardanti, ad esempio, il fatto che i requisiti di legge siano sufficientemente accessibili, precisi e prevedibili nell'applicazione, necessari o proporzionati per il loro (legittimo/fondamentale) scopo.

Si tratta di problemi che non possono essere risolti, nè trattati, tramite "meccanismi di cooperazione e coerenza" di cui parleremo in seguito, perchè questi meccanismi si limitano alla cooperazione su misure che le autorità di protezione dei dati hanno già avviato o intendono avviare e non possono essere utilizzati per porre rimedio alle carenze legislative degli Stati membri. Si tratta, però, di una situazione che può causare seri problemi, in particolare a livello del trasferimento dei dati personali da un'agenzia di Stato in uno Stato membro dell'UE ad un'altra agenzia in un altro Stato membro, soprattutto se in quest'ultimo i dati fossero trattati secondo norme non conformi ai requisiti di legge. Esperienze in altri ambiti normativi (come quello della Giustizia e degli Affari interni, non trattato in questa prima edizione del Manuale) dimostrano comunque che possono essere presi i provvedimenti necessari per affrontare tali questioni, soprattutto sulla base dei suggerimenti e delle proposte della Commissione o del Comitato europeo per la protezione dei dati.

Conseguenze per i RPD

Da quanto sinora detto emerge chiaramente che i RPD debbano ben conoscere, e **studiare, non solo i dispositivi del RGPD, ma anche le norme nazionali che si fondano sulle "clausole di specificazione" del RGPD** – nonché tutte le leggi e le norme attinenti in altri Stati membri e in paesi terzi, qualora l'organizzazione per la quale lavorino divulghi dati personali a tali Stati.

Queste realtà possono assumere svariate forme. In alcuni casi, gli Stati membri possono semplicemente aver mantenuto nei loro ordinamenti disposizioni precedenti all'entrata in vigore del RGPD, comprese deroghe speciali per tutelare interessi pubblici vitali o facilitare la ricerca – sebbene tali **disposizioni non abbiano, magari, mai rispettato i requisiti prima ricordati delle rispettive "clausole di specificazione" o non siano "adeguate" o "idonee" ai sensi del RGPD** (come visto in precedenza). In altri casi, lo Stato membro potrebbe aver adottato normative specifiche per "regolamentare ulteriormente" questioni di sua iniziativa ai sensi del RGPD, o dover chiarire quali opzioni sono state scelte, ecc. In altri casi ancora, lo Stato membro potrebbe non aver chiarito per nulla l'applicazione nazionaledi delle pertinenti "clausole di specificazione".

Non è certamente compito dei RPD colmare qualsiasi lacuna in materia. E' altresì vero, però, che grazie alla rete dei colleghi e alle interazioni con le rispettive autorità nazionali di

230 Si veda: Douwe Korff, *The question of "applicable law"*, in: Guida per la conformità 3 – Relazione ad interim, Privacy Laws & Business, novembre 1999.

protezione dei dati,[231] i RPD possono **farsi propugnatori di inizative e incoraggiare azioni concrete**. Inoltre possono, preferibilmente con la collaborazione di altri RPD che lavorano in organizzazioni simili, **avvisare e sensibilizzare le alte gerarchie delle rispettive organizzazioni** (nel settore pubblico, ad esempio, i Ministri di governo dei settori interessati) su tali lacune e sviluppare approcci strategici ed efficaci.

2.3 Panoramica sul RGPD

Qui di seguito una panoramica capitolo per capitolo, sezione per sezione e articolo per articolo del RGPD.*

*Sperabilmente, la prossima e più ampia edizione del presente Manuale recherà un breve commentario, articolo per articolo, di tutte le disposizioni del RGPD, focalizzato sull'applicazione pratica e concreta delle sue disposizioni. Per adesso, consigliamo ai RPD di consultare una delle numerose opere di commento pubblicate nei singoli Paesi, oltre ovviamente agli orientamentli ufficiali pubblicati dalle autorità nazionali di controllo, dal Comitato europeo e dagli organi giudiziari.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI
CAPO I: **Disposizioni generali**
Art. 1: **Oggetto e finalità**
Art. 2: **Ambito di applicazione materiale**
Art. 3: **Ambito di applicazione territoriale**
Art. 4: **Definizioni**
CAPO II: **Principi**
Art. 5: **Principi applicabili al trattamento dei dati personali**
Art. 6: **Liceità del trattamento [basi giuridiche]**
Art. 7:

[231] Cfr. l'"Extranet" del RPD **francese** per la sua utilità in tale contesto. Si veda p. 146, *supra*.

Condizioni per il consenso
Art. 8: **Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione**
Art. 9: **Trattamento di categorie particolari di dati personali**
Article 10: **Trattamento dei dati personali relativi a condanne penali e reati**
Art. 11: **Trattamento che non richiede l'identificazione**
CAPO III: **Diritti dell'interessato**
Sezione 1: **Trasparenza e modalità**
Art. 12: **Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato**
Sezione 2: **Informazione e accesso ai dati personali**
Art. 13: **Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato**
Art. 14: **Informazioni da fornire qualora i dati personali non siano ottenuti presso l'interessato**
Art. 15: **Diritto di accesso dell'interessato**
Sezione 3: **Rettifica e cancellazione**
Art. 16: **Diritto di rettifica**
Art. 17:

Diritto alla cancellazione ('diritto all'oblio')
Art. 18: **Diritto di limitazione di trattamento**
Art. 19: **Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento**
Art. 20: **Diritto alla portabilità dei dati**
Sezione 4: **Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche**
Art. 21: **Diritto di opposizione**
Art. 22: **Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione**
Sezione 5: **Limitazioni**
Art. 23: **Limitazioni**
CAPO IV: **Titolare del trattamento e responsabile del trattamento**
Sezione 1: **Obblighi generali**
Art. 24: **Responsabilità del titolare del trattamento**
Art. 25: **Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita**
Art. 26: **Contitolari del trattamento**
Art. 27:

Rappresentanti dei titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione
Art. 28: **Responsabile del trattamento**
Art. 29: **Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento**
Art. 30: **Registri delle attività di trattamento**
Art. 31: **Cooperazione con l'attività di controllo**
Sezione 2: **Sicurezza del trattamento**
Art. 32: **Sicurezza del trattamento**
Art. 33: **Notifica di una violazione dei dati personali all'autorità di controllo**
Art. 34: **Comunicazione di una violazine dei dati personali all'interessato**
Sezione 3: **Valutazione d'impatto sulla protezione dei dati e consultazione preventiva**
Art. 35: **Valutazione d'impatto sulla protezione dei dati**
Art. 36: **Consultazione preventiva**
Sezione 4: **Responsabile della protezione dei dati**
Art. 37: **Designazione del responsabile della protezione dei dati**

Art. 38: **Posizione del responsabile della protezione dei dati**
Art. 39: **Compiti del responsabile della protezione dei dati**
Sezione 5: **Codici di condotta e certificazione**
Art. 40: **Codici di condotta**
Art. 41: **Monitoraggio dei codici di condotta approvati**
Art. 42: **Certificazione**
Art. 43: **Organismi di certificazione**
CAPO V: **Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali**
Art. 44: **Principio generale per il trasferimento**
Art. 45: **Trasferimento sulla base di una decisione di adeguatezza**
Art. 46: **Trasferimento soggetto a garanzie adeguate**
Art. 47: **Norme vincolanti d'impresa**
Art. 48: **Trasferimento o comunicazione non autorizzati dal diritto dell'Unione**
Art. 49: **Deroghe in specifiche situazioni**
Art. 50: **Cooperazione internazionale per la protezione dei dati personali**
CAPO VI: **Autorità di controllo indipendenti**
Sezione 1:

Independenza
Art. 51: **Autorità di controllo**
Art. 52: **Independenza**
Art. 53: **Condizioni generali per i membri dell'autorità di controllo**
Art. 54: **Norme sull'istituzione dell'autorità di controllo**
Sezione 2: **Competenza, compiti e poteri**
Art. 55: **Competenza**
Art. 56: **Competenza dell'autorità di controllo capofila**
Art. 57: **Compiti**
Art. 58: **Poteri**
Art. 59: **Relazioni di attività**
CAPO VII: **Cooperazione e coerenza**
Sezione 1: **Cooperazione**
Art. 60: **Cooperazione fra l'autorità di controllo capofila e le autorità di controllo interessate**
Art. 61: **Assistenza reciproca**
Art. 62: **Operazioni congiunte delle autorità di controllo**
Sezione 2: **Coerenza**

Art. 63: **Meccanismo di coerenza**
Art. 64: **Parere del comitato europeo per la protezione dei dati**
Art. 65: **Composizione delle controversie da parte del comitato**
Art. 66: **Procedura d'urgenza**
Art. 67: **Scambio di informazioni**
Sezione 3: **Comitato europeo per la protezione dei dati**
Art. 68: **Comitato europeo per la protezione dei dati**
Art. 69: **Indipendenza**
Art. 70: **Compiti del comitato**
Art. 71: **Relazioni**
Art. 72: **Procedura**
Art. 73: **Presidente**
Art. 74: **Compiti del presidente**
Art. 75: **Segreteria**
Art. 76: **Riservatezza**
CAPO VIII: **Mezzi di ricorso, responsabilità e sanzioni**
Art. 77:

Diritto di proporre reclamo all'autorità di controllo
Art. 78: **Diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo**
Art. 79: **Diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento**
Art. 80: **Rappresentanza degli interessati**
Art. 81: **Sospensione delle azioni**
Art. 82: **Diritto al risarcimento e responsabilità**
Art. 83: **Condizioni generali per infliggere sanzioni amministrative pecuniarie**
Art. 84: **Sanzioni**
CAPO IX: **Disposizioni relative a specifiche situazioni di trattamento**
Art. 85: **Trattamento e libertà d'espressione e di informazione**
Art. 86 **Trattamento e accesso del pubblico ai documenti ufficiali**
Art. 87: **Trattamento del numero di identificazione nazionale**
Art. 88: **Trattamento dei dati nell'ambito dei rapporti di lavoro**
Art. 89: **Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici**
Art. 90: **Obblighi di segretezza**
Art. 91: **Norme di protezione dei dati vigenti presso chiese e associazioni religiose**

CAPO X: **Atti delegati e atti di esecuzione**
Art. 92: **Esercizio della delega**
Art. 93: **Procedura del comitato**
CAPO XI: **Disposizioni finali**
Art. 94: **Abrogazione della Direttiva 95/46/CE**
Art. 95: **Rapporto con la Direttiva 2002/58/CE**
Art. 96: **Rapporto con accordi precedentemente conclusi**
Art. 97: **Relazioni della Commissione**
Art. 98: **Riesame degli altri atti legislativi dell'Unione in materia di protezione dei dati**
Art. 99: **Entrata in vigore e applicazione**

2.4 Il principio di responsabilizzazione[232]

2.4.1. Il nuovo obbligo di dimostrazione della conformità

Benché possa anche non sembrare una novità, (e in effetti si potrebbe affermare che trae ispirazione dal modello americano, a sua volta trasposto nelle linee-guida OCSE del 1980) si tratta di una delle caratteristiche principali del Regolamento generale sulla protezione dei dati dell'EU (RGPD) – anzi, forse *la* caratteristica principale – che enfatizza e ribadisce che:

> **Il titolare del trattamento è competente per ed *è in grado di comprovare il rispetto dei* [principi applicabili al trattamento dei dati personali] («responsabilizzazione»)** (Art. 5(2)).

[232] Questa sezione si rifà, in parte ripetendolo e riassumendolo, al testo di Douwe Korff, The Practical Implications of the new EU General Data Protection Regulation for EU- and non-EU Companies, agosto 2016, documento presentato al CMS Cameron McKenna LLP, Londra, nel febbraio 2017, disponibile su: http://ssrn.com/abstract=3165515

Come afferma l'autorità italiana della protezione dei dati, il *Garante della Privacy*,:[233]

> *Responsabilizzare* un'entità significa attribuirle azioni e decisioni **e aspettarsi che ne renda conto**. In questo senso, la responsabilizzazione è **l'essere tenuti a rispondere** delle azioni e delle decisioni che ci competono.

La novità risiede non tanto nell'Autorità responsabile del trattamento e della sua conformità - un caso di specie già ben identificato dalla Direttiva sulla protezione dei dati personali del 1995 (sebbene questo testo non utilizzasse il termine di "responsabilizzazione"),- quanto, piuttosto, nell'accento posto sul titolare e, in alcuni casi, sul responsabile del trattamento, che hanno il dovere di "**dimostrare**" la conformità: nel Regolamento questo termine figura non meno di 33 volte.

La differenza con la Direttiva sulla protezione dei dati personali del 1995, la quale in nessuna delle sue disposizioni richiedeva a un titolare o ad un responsabile di dimostrare alcuna ottemperanza (salvi gli obblighi imposti da un'autorità di controllo o da un autorità giudiziaria), è quindi evidente. Più in dettaglio, i vari schemi di "notifica" o "registrazione" della Direttiva non sono serviti a molto, almeno in alcuni paesi, per dimostrare il rispetto della conformità,[234] mentre in altri hanno ottenuto un successo maggiore, ma solo grazie all'estrema articolazione normativa, all'essere stati presentati in modo tale da orientare i titolari ad applicare i requisiti di legge a qualsiasi nuova operazione riguardante il trattamento dei dati e al ruolo di segnalazione al titolare svolto dalle DPA interessate (che si sono anche attivate nel proporre modifiche e formulare pareri dove richiesto o necessario). In un contesto di prassi in materia di trattamento dei dati che si evolvono e prendono piede con grande rapidità, ed in paesi (come gli Stati membri dell'UE) che già vantano conoscenze ed esperienze significative nell'applicazione delle normative e dei principi sulla protezione dei dati, visto anche il contesto di promozione della "responsabilità sociale" delle varie organizzazioni, era veramente necessario un nuovo approccio che mettesse in rilievo la responsabilità primaria e la responsabilizzazione di coloro (titolari o responsabili) che si occupano del trattamento dei dati. Il principio di responsabilizzazione e l'obbligo di conformità rispondono a questo bisogno.

Come vedremo nella sezione 2.3, *infra*, il Regolamento prevede, quale mezzo principale per mettere in pratica il principio di responsabilizzazione, la nomina di responsabili della protezione dei dati (RPD) per tutti i settori pubblici, e per molti di quelli privati.

Come stabilisce chiaramente il principio di responsabilizzazione all'Art. 5(2), di cui sopra, il dovere di dimostrare la conformità si applica prima di tutto ai principi di base che sottendono il Regolamento, e di cui all'Art. 5(1), vale a dire liceità, correttezza e trasparenza; identificazione precisa e circostanziata del tipo e della limitazione delle finalità; minimizzazione dei dati (che devono essere adeguati, pertinenti e limitati); esattezza (compreso l'aggiornamento); limitazione della conservazione; integrità, riservatezza e sicurezza. Naturalmente, tali norme sono ancora più vincolanti e, *a fortiori,* applicabili al trattamento di particolari categorie di dati (i cosidetti dati sensibili di cui all'Art. 9) o a trattamenti che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche (e per questo richiedono una valutazione d'impatto specifica sulla protezione dei dati – Art. 35).

---

233 Luigi Carrozzi, presentazione alla prima sessione di formazione "T4DATA", giugno 2018, schermata relativa a "*Inventario dei beni e principio di responsabilizzazione*" (grassetto in originale).

234 Si veda il RGPD, Considerando 89.

Inoltre, il Regolamento impone, in modo evidente oppure implicito, l'obbligo di dimostrazione della conformità anche in contesti più specifici, come:

- L'ottenimento del consenso (quando richiesto) (si veda Art. 7(1));
- il rifiuto di una richiesta da parte di un interessato di accesso o rettifica dei dati (si vedano gli Art. 11(2) e 12(5));
- l'astensione dal trattamento in caso di opposizione dell'interessato (si veda l'Art. 21(1));
- l'esistenza di "garanzie sufficienti" in termini di competenza e la messa in atto di "misure tecniche ed organizzative" per garantire la sicurezza del trattamento dei dati da parte dei responsabili e dei sotto-responsabili (si vedano gli Art. 28 e 32);
- l'esistenza di "garanzie adeguate" per il trasferimento dei dati personali a paesi terzi privi di garanzie adeguate (Art. 46);
- eccetera.

Strettamente correlate all'obbligo di dimostrabilità della conformità, sono poi le norme, generali e specifiche, che il RGPD impone in materia di

- **creazione di un registro dei trattamenti di dati personali;**
- **conduzione di un'analisi complessiva di tali trattamenti;**
- **valutazione dei rischi per i diritti e le libertà delle persone fisiche derivanti da tali trattamenti;**
- **effettuazione di approfondite valutazioni di impatto sulla protezione dei dati in rapporto a trattamenti che la valutazione mostri poter comportare un "rischio elevato";**
- **applicazione dei principi di protezione dei dati fin dalla fase di progettazione e per impostazione predefinita con riguardo a tutti i trattamenti di dati personali;**
- **obblighi di notifica delle violazioni dei dati personali**.

Esamineremo tutti questi aspetti, e in particolare il ruolo spettante al RPD in questo ambito, nella Parte III. In questa sede ci limiteremo ad alcuni brevi cenni facendo rinvio alla Parte III.

Prima di tutto, il regolamento impone un **obbligo generale fondamentale di tenuta di registri dettagliati delle attività di trattamento dei dati personali effettuate dal titolare**, specificando i dettagli di ogni singola attività (Art. 30); i registri devono dimostrare come e in che modo si è attuata la conformità a quanto stabilito dal Regolamento sia in materia di obblighi generali che specifici (cfr. Considerando 82). Si vedano le considerazioni svolte rispetto al Compito 1 nella Parte III del Manuale.

In secondo luogo, il Regolamento impone ai titolari, con l'aiuto dei RPD, di analizzare i trattamenti svolti e, ove necessario, renderli conformi al Regolamento stesso, indicando nel suddetto registro le attività di analisi e le misure correttive adottate. Si vedano le considerazioni svolte rispetto al Compito 2 nella Parte III del Manuale.

In terzo luogo, il Regolamento impone al titolare del trattamento l'obbligo generale di "tenere conto" dei **rischi** inerenti alle operazioni di trattamento da lui effettuate, l'obbligo di attuare "misure tecniche ed organizzative adeguate" per minimizzare tali rischi, nonché quello di

"dimostrare che il trattamento è effettuato conformemente al Regolamento" – ossia, il Regolamento impone l'obbligo di effettuare una valutazione dei rischi e di adottare misure adeguate a tali rischi (Art. 24(1); si veda anche l'Art. 32) . Anche di questi elementi deve restare traccia: si vedano in proposito le considerazioni svolte rispetto al Compito 3 nella Parte III del Manuale.

In quarto luogo, se la valutazione del rischio (di cui sopra) dimostra la probabilità di un **rischio elevato** per i diritti e le libertà della persona fisica, il titolare ha l'obbligo, prima del trattamento, di effettuare una **valutazione di impatto dei trattamenti previsti sulla protezione dei dati (DPIA)**, e di **documentare** tale valutazione. Nello specifico, tale documentazione deve contenere: una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento; una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; una valutazione del rischio che il trattamento comporta per i diritti e le libertà degli interessati; una descrizione delle misure previste per affrontare tali rischi incluse "*le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e* ***dimostrare*** *la conformità al presente Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione"* (Art. 35). Si vedano le considerazioni svolte rispetto al Compito 4 nella Parte III del Manuale.

In quinto luogo, il Regolamento impone ai titolari del trattamento un obbligo generale di utilizzo della "**Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (Data Protection-by-Design and-Default)**", sia nella fase di progettazione che di esecuzione delle attività di trattamento del titolare (Art. 25) – e al titolare compete dimostrare l'ottemperanza di tali norme. A tale proposito, il Regolamento stabilise che un meccanismo di certificazione (marchio di qualità della protezione dei dati) può essere utilizzato come un "elemento" per dimostrare la conformità (Art. 25(3), di cui riparleremo in seguito). Si vedano le considerazini svolte rispetto al Compito 9 nella Parte III del Manuale

In sesto luogo, i titolari devono **documentare nel dettaglio** qualsiasi violazione dei dati personali (violazione della sicurezza dei dati), i provvedimenti adottati per porvi rimedio e **notificare le violazioni** alle competenti Autorità di controllo entro 72 ore (Art. 33). Anche gli interessati devono essere informati della violazione, anche se meno dettagliatamente e solo qualora la violazione "sia suscettibile di presentare un elevato rischio per i diritti e le libertà delle persone fisiche" (Art. 34). Si vedano le considerazioni svolte rispetto al Compito 6 nella Parte III del Manuale.

Il Regolamento contiene anche dispositivi più specifici sugli obblighi di registrazione, fra cui la previsione per cuiquando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. In quanto tali, "determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente Regolamento" sotto forma di un "**accordo**" che deve "riflettere adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati". Nella pratica, poiché le Autorità di controllo possono chiedere ai titolari l'osservanza delle norme stabilite, l'accordo deve essere messo **per iscritto o in un formato elettronico comparabile e attendibile** (Art. 26).

Vi sono poi ovviamente le varie disposizioni del Regolamento che impongono a titolari, co-titolari, responsabili e sub-responsabili di specificare i reciproci obblighi e rapporti, anche con riguardo a trasferimenti di dati, attraverso contratti o analoghi strumenti giuridicamente vincolanti. Di tutto ciò occorre serbare documentazione.

2.4.2. Mezzi di dimostrazione della conformità

L'obbligo generale di mantenere **registrazioni dettagliate**, e i doveri più specifici di registrazione imposti ai contitolari del trattamento, denuncia delle violazioni e DPIA, di cui sopra, rappresentano i principali mezzi di dimostrazione della conformità fissati dal Regolamento.

Per riflettere una cultura ed un approccio generale finalizzati alla promozione della protezione dei dati, il rispetto delle disposizioni normative dovrebbe richiedere l'adozione di **misure pratiche** quali:

- l'adozione e l'attuazione formale di politiche interne sulla protezione dei dati (ed azioni correlate, come la formazione);
- l'incorporazione dei principi della protezione dei dati by design e by default in tutte le attività di trattamento, i prodotti e i servizi del titolare, in ogni fase che va dalla progettazione alla messa in opera;
- la riduzione al minimo dell'uso e della conservazione dei dati personali e, più specificamente, l'utilizzo di dati ancora tracciabili ed identificabili (ricorrendo alla pseudonimizzazione o all'anonimizzazione di tali dati, nella misura del possibile);
- la garanzia della piena trasparenza sull'attività di trattamento del titolare nei confronti dell'interessato e del pubblico più in generale, in forma cartacea, via web, in dichiarazioni chiare e più dettagliate sulla protezione dei dati /della privacy sui siti web, (che, ad esempio, visualizzino in modo inequivoco e diretto sulla pagina web le fonti da cui i dati personali sono raccolti, i dati e le finalità obbligatorie rispetto a quelle opzionali, e offrano una maggiore legittimità di scelta agli utenti con un semplice click su una casella), e attuando meccanismi efficaci ed efficienti per l'informazione, generale e specifica, dell'interessato; inoltre
- la garanzia che il titolare possa continuare a monitorare direttamente le attività, in particolare quelle attinenti alla sicurezza (con adeguati mezzi di accesso e alterazione dei log, ecc., oppure migliorando la sicurezza dove necessario, ad es. emettendo "patch").

  (Cfr. Considerando 78)

Nella Terza Parte, riprenderemo e approfondiremo questi elementi con esempi pratici e specifici per risolvere e affrontare le varie questioni emerse.

Per completezza, il precedente Considerando (77) fornisce una lista di **misure speciali** che permettono di dimostrare le conformità, ad es.:

- agire secondo codici di condotta approvati;
- agire secondo certificazioni sulla protezione dei dati approvate;
- agire secondo linee guida elaborate dal Comitato europeo per la protezione dei dati;

  e naturalmente:

- agire secondo le indicazioni di un RPD.

Se parliamo anche di trasferimento transfrontaliero di dati e di condivisione di dati personali potremmo senz'altro aggiungere:

- le norme vincolanti d'impresa (BCR);
- gli accordi amministrativi ("arrangements") fra autorità o organismi pubblici; e
- i contratti standard o stipulati individualmente di trasferimento dei dati.

In relazione alla violazione dei dati, poi, anche la notifica (ed i dettagli in essa contenuta) può costituire un mezzo valido per dimostrare la conformità ad un requisito di legge.

Tuttavia, occorre sottolineare che le misure sopra ricordate, pur rappresentando "elementi" di un approccio complessivamente orientato a dimostrare la conformità, anche attraverso alcune "misure speciali", non forniscono necessariamente evidenza probatoria di tale conformità.

2.4.3 Valore probatorio delle misure per la dimostrazione della conformità

Da molti punti di vista, l'adesione ad una delle misure di conformità costituisce un "elemento che permette la dimostrazione della conformità", ad es., creando una presunzione relativa di conformità. Se un'Autorità sulla protezione dei dati dovesse ulteriormente indagare la questione, potrebbe emergere che, per una specifica fattispecie e nonostante l'adesione formale a linee guida, codici, certificati, accordi, contratti o norme, il Regolamento non è mai stato rispettato (sebbene ogni sforzo fatto in buona fede per ottemperarvi avrebbe naturalmente un impatto significativamente positivo a livello sanzionatorio, qualora sanzioni fossero di applicazione – cfr. Art. 83).

2.5 Il Responsabile della protezione dei dati (RPD)

2.5.1 Contesto generale

La figura di un responsabile della protezione dei dati, di nomina pubblica o privata, deriva dalla legislazione tedesca sulla protezione dei dati, nella cui normativa tale figura compare da tempo.[235] Anche in Paesi che, ai sensi della Direttiva sulla protezione dei dati personali del 1995 non hanno proceduto alla nomina, per legge, di un RDP - Responsabile dei dati personali (come l'Austria, che da molti punti di vista segue sempre da vicino l'esempio tedesco), o che hanno introdotto tale designazione solo in via opzionale (come la Francia), questa figura è stata spesso ampiamente adottata. In molti paesi esistono associazioni nazionali di RPD ed esiste anche una Confederazione europea dei responsabili della protezione dei dati, CEDPO, che ha eleborato "linee-guida pratiche destinate alle organizzazioni" sulla "scelta del miglior candidato" per la carica di RPD.[236] A livello globale, esiste poi l'Associazione Internazionale

---

235 I termini tedeschi sono rispettivamente: *behördliche* e *betriebliche Datenschutzbeauftragter*. Per un breve riassunto del ruolo e delle funzioni dei RPD nel diritto tedesco, si veda: https://www.wbs-law.de/eng/practice-areas/internet-law/it-law/data-protection-officer/
Per maggiori dettagli, in lingua tedesca, si veda, ad es., Däubler/Klebe/Wedde/Weichert, Kompaktkommentar zum BDSG (Breve commento alla Legge federale sulla protezione dei dati), 3^ed. (2010), commenti al §4f BDSG, comprese le 85 note a margine, pp. 187 – 213.

236 CEDPO, Choosing the best candidate as your Data Protection Officer (DPO) – Practical guidelines for organisations, 30 maggio, disponibile su: http://businessdocbox.com/Human_Resources/77901620-Choosing-the-best-candidate-as-your-data-protection-officer-dpo-practical-guidelines-for-organisations.html

dei Professionisti della Privacy (IAPP), con sede negli USA, che, *inter alia,* rilascia certificazioni sulla protezione dei dati per i "professionisti della privacy informazionale" – anche se, come altri schemi di certificazione relativi alla figura del RPD, non si tratta di certificati di conformità fondati sul RGPD: si veda la sezione 2.5.3, *infra*, alla voce "Formazione e certificazione".

(Si veda la lista delle Associazioni dei RPD alla fine di questa sottorubrica ed i link ai rispettivi siti web).

La Direttiva sulla protezione dei dati del 1995 non obbligava ancora alla nomina di RPD da parte dei titolari del trattamento. Riconosceva, invece, l'esistenza dei RPD nelle prassi e nelle normative degli Stati membri offrendo loro la possibilità di esentare i titolari dall'obbligo di notifica delle operazioni di trattamento alle Autorità nazionali di protezione dei dati di riferimento (DPA) qualora la legislazione dello Stato membro imponesse al titolare la nomina di un RPD "*responsabile, in particolare [ ], di vigilare in maniera indipendente all'osservanza interna delle disposizioni nazionali adottate ai sensi di questa direttiva [e] al mantenimento di [un] registro delle attività di trattamento eseguite dal titolare in cui figurino [le stesse informazioni che sarebbero state notificate alla DPA]*" (Art. 18(2)).

Teniamo presente che il Regolamento 2001 UE, che fissava le norme per la protezione dei dati per le stesse istituzioni europee (Regolamento (CE) 45/2001),[237]obbliga ciascuna istituzione o organismo dell'UE alla nomina di almeno un RPD (Art. 24). Le disposizioni di questo Regolamento, e applicabili ai RPD delle istituzioni europee, sono molto simili a quelli del RGPD.

La Direttiva di protezione dei dati personali (Direttiva di Polizia), (Direttiva 2016/680),[238] adottata nello stesso periodo del RGPD, stabilisce che anche "le autorità competenti" subordinate alla Direttiva nominino un RPD; e le Linee guida sui RPD del WP29 (che, come vedremo fra poco, contengono le norme principali per la nomina dei RPD ai sensi del RGPD) sottolineano che "mentre queste linee guida si incentrano sui RPD ai sensi del RGPD, tali indicazioni, per disposizioni analoghe, sono assolutamente pertinenti ai RPD ai sensi della Direttiva 2016/680".[239]

I RPD dell'Unione Europea lavorano in stretta collaborazione con il Garante europeo della protezione dei dati (GEPD) e hanno dato vita a una Rete di Responsabili della protezione dei dati delle Istituzioni e degli Organismi dell'UE. Il GEDP ha creato, per facilitarne il lavoro, un

---

237 Titolo completo: Regolamento (CE) N° 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati , GU L 8 del 12.1.2001, p. 1 e ss., consultabile su:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001R0045&from=EN

238 Titolo completo: 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, GU L 119, 4.5.2016, p. 89 e ss., disponibile su:
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN

239 Gruppo di lavoro Articolo 29 Linee guida sui Responsabili della protezione dei dati ('RPD'), adottato originariamente il 13 dicembre 2016, ultima revisione e adozione finale il 5 aprile 2017 (WP243 rev.01), p. 4, nota 2.:
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048
Da qui in avanti faremo riferimento a questo testo come "**Le linee guida sui DPO del WP29**".

sito web, l'"Angolo del RPD". Dopo un documento del 2005 del GEPD,[240] nel 2010, la Rete ha dato alle stampe le Qualifiche professionali per i RPD delle Istituzioni e degli Organismi dell'UE che lavorano ai sensi del Regolamento (CE) 45/2001 (Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001).[241] Nel 2012, il GEPD ha elaborato una relazione sullo statuto dei RPD, come parte dell'attività di monitoraggio, da parte delle istituzioni, della conformità al Regolamento (CE) 45/2001.[242]La relazione conferma che "la funzione di RPD è ben consolidata nelle istituzioni e negli organismi europei e che, in genrale, ottempera all'Art. 24 del Regolamento", ma rileva anche "alcuni ambiti di preoccupazione" che devono essere oggetto di ulteriore monitoraggio da parte del GEPD.[243] Questi documenti contengono linee guida molto articolate su importanti questioni quali la nomina, la posizione ed i compiti dei RPD.

Più di recente, e di maggiore interesse per questo Manuale, il Gruppo di lavoro Articolo 29 (WP29) ha elaborato "Linee guida sui RPD (testo in preparazione per la piena applicazione del RGPD)".[244] Il Comitato Europeo per la protezione dei dati, che ha sostituito il WP29 dopo l'applicazione del RGPD, ha approvato formalmente queste linee guida (e altri documenti relativi a problematiche del RGPD, adottati dal WP29 prima di questa data).[245]

Numerose DPA nazionali, di conseguenza, hanno elaborato guide sui RPD, alcune anche prima del RGPD, e promosso servizi specifici a loro favore.[246]

Questa parte del Manuale attinge, in particolare, alle linee guida del WP29, ma fa anche riferimento, quando necessario per un ulteriore arricchimento, ad altri testi esplicativi di cui abbiamo già parlato.

L'elemento cruciale da sottolineare in questa introduzione al RPD è che, ai sensi del RGPD, si tratta di una figura completamente nuova che costituisce uno strumento fondamentale per

---

240 EDPS, Documento di posizione sul ruolo dei Responsabili della protezione dei dati nel rispetto della conformità con il Regolamento (CE) 45/2001:
https://edps.europa.eu/sites/edp/files/publication/05-11-28_dpo_paper_en.pdf

241 https://edps.europa.eu/sites/edp/files/publication/10-10-14_dpo_standards_en.pdf

242 EDPS, Monitoraggio della conformità delle Istituzioni e degli Organismi europei all'Art. 24 del Regolamento (CE) 45/2001 – Relazione sullo statuto dei RPD, 17 dicembre 2012:
https://edps.europa.eu/sites/edp/files/publication/2012-12-17_dpo_status_web_en.pdf

243 *Idem*, p. 3.

244 Si veda nota 239, *supra*.

245 EDPB, Approvazione 1/2018, con approvazione, *inter alia,* delle Linee-guida sui DPO del WP29 (figurante al 7° documento approvato), adottata il 25 maggio 2018:
https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf

246 Si veda, ad es.:
Guide de Correspondant Informatique et Libertés (CIL) (*Guide Pratique Correspondant*), dell'autorità **francese** della protezione dei dati, CNIL, 2011:
https://www.cnil.fr/sites/default/files/typo/document/CNIL_Guide_correspondants.pdf
In **Italia**, l'Autorità nazionale di protezione dei dati, il *Garante della Privacy*, ha pubblicato un elenco di domande frequenti (FAQ) sui RPD:
https://www.garanteprivacy.it/garante/doc.jsp?ID=8036793 (FAQ sui RPD nel settore privato)
https://www.garanteprivacy.it/garante/doc.jsp?ID=7322110 (FAQ sui RPD nel settore pubblico)
Nel Regno Unito, l'autorità nazionale sulla protezione dei dati, la *Information Commissioner* (solitamente denominata ICO, acromino di Information Commissioner's Office), offre sul proprio sito web linee guida che riflettono, e rimandano, sostanzialmente, a quelle del WP29:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

garantire efficacia pratica al principio di "responsabilizzazione" (obbligo di dimostrazione della conformità) di cui abbiamo già avuto modo di parlare: la nomina di un RPD e la scrupolosa esecuzione dei compiti che lo attendono (come fatto notare nella Terza Parte di questo Manuale), dovrebbero garantire una conformità alle disposizioni del RGPD migliore, più completa e scupolosa rispetto a quella ottenuta, prevalentemente, dalla supervisione esterna esercitata dalle autorità della protezione dei dati ai sensi della Direttiva sulla protezione dei dati del 1995. Oggi, grazie alle norme del RGPD, le DPA si possono avvalere sia di un punto di contatto noto e diretto, che di un alleato. Non sorprende, quindi, che molte DPA ne abbiano fatto una figura prioritaria, adesso che il RGPD è divenuto pienamente applicabile, e verifichino se le organizzazioni che hanno l'obbligo di nominare un RPD (come vedremo alla sezione 2.3.2) abbiano proceduto in tal senso.[247]

ASSOCIAZIONI INTERNAZIONALI E NAZIONALI DEI RESPONSABILI DELLA PROTEZIONE DEI DATI (RPD):

Associazioni internazionali:

Mondiali:

International Association of Privacy Professionals (IAPP):
https://iapp.org/certify/cipp/

Europee;

Network of Data Protection Officers of the EU Institutions and Bodies:
https://edps.europa.eu/data-protection/eu-institutions-dpo_en

Confederation of European Data Protection Organisations, CEDPO
http://www.cedpo.eu/

Associazioni nazionali:
(Quelle contrassegnate con l'asterisco* fanno parte del CEDPO)

Francia:
Association Française des Correspondants à la Protection des Données à Caractère Personnel, AFCDP:*
https://www.afcdp.net/

Irlanda:
Association of Data Protection Officers, ADPO:*
https://www.dpo.ie/

Italia:
Associazione Data Protection Officer, ASSO DPO:*

[247] Per citare un esempio, la DPA **svedese** ha annunciato uno studio per verificare se i settori bancari, sanitari ed assicurativi abbiano nominato un RPD:
https://www.datainspektionen.se/nyheter/datainspektionen-inleder-forsta-granskningarna-enligt-gdpr/
Anche la DPA **dei Paesi Bassi** rileva, nel suo piano di lavoro 2018 – 2019, *in particolare per quanto riguarda le relazioni con le autorità pubbliche*, che verificherà: "*la conformità all'obbligo di mantenimento di un registro dei trattamenti, della nomina di un RPD, del rispetto della posizione dello stesso in seno all'organizzazione e di realizzazione dei compiti attribuiti alla sua carica ai sensi del RGPD*", si veda:
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/toezichtkader_autoriteit_persoonsgegevens_2018-2019.pdf [p. 7, al capitolo"*Overheid*" (autorità pubblica), traduzione nostra].

http://www.assodpo.it/en/home_en/

Paesi Bassi:
Nederlands Genootschap voor Functionarissen Gegevensbescherming, NGFG:*
https://www.ngfg.nl/

Polonia:
Stowarzyszenie Administratorów Bezpieczeństwa Informacji, SABI:*
http://www.sabi.org.pl/

Spagna
Asociación Profesional Española de Privacidad, APEP:*
http://www.apep.es/

Regno Unito:
National Association of Data Protection & Freedom of Information Officers, NADPO:
https://nadpo.co.uk/

I Membri di **Germania** ed **Austria** del CEDPO, rispettivamente il *Gesellschaft für Datenschutz und Datensicherheit e.V.*, DGG* (fondato nel 1977) e *Arge Daten**, raggruppano non solo RPD, ma fanno entrambi parte del CEDPO:
https://www.gdd.de/ueber-uns
http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=15904tpb

2.5.2 L'obbligo di nomina di un RPD per le autorità pubbliche[248]

La nomina di un RPD è obbligatoria per tutte le autorità pubbliche o gli organismi che trattano dati personali che rientrano nel campo di applicazione del Regolamento (Art. 37(1)(a)).[249]Anche se tale nomina è di competenza degli Stati membri, il WP29, a ragione, interpreta questa disposizione in modo piuttosto ampio:[250]

---

[248] Ad eccezione di organismi privati che svolgono "compiti pubblici" o "esercitano un'autorità pubblica"– come già visto nel testo – l'obbligo di nomina di un RPD per aziende "a carattere puramente privato" (commerciale) non è oggetto di discussione nel presente Manuale. Basti osservare che, per tali istanze, il Regolamento obbliga alla nomina, in principio, di un RPD allorquando:

- 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
- 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 [i cosidetti dati personali] o di dati relativi a condanne penali e a reati di cui all'articolo 10. (Articolo 37(1)(b) e (c) RGPD).

Queste norme sono discusse dettagliatamente nelle Linee-guida per i DPO del WP29. Basti qui ricordare che, in pratica, molte aziende grandi e piccole ritengono che la nomina di un RPD sia utile per ottemperare ai principi di "responsabilizzazione"/ "dovere di dimostrazione della conformità" di cui abbiamo parlato al punto 2.2.

[249] L'unica eccezione riguarda le "autorità giurisdizionali nell'esercizio delle loro funzioni" (Art. 37(1)(a) RGPD). In ogni caso, come il WP29 sottolinea nelle sue Linee guida ai RPD (nota precedente), questo non significa che tali autorità non debbano ottemperare al Regolamento, al contrario. Per quanto riguarda, poi, il trattamento dei dati da parte di autorità giurisdizionali nell'esercizio diverso da quello delle loro funzioni, hanno comunque l'obbligo di nominare un RPD.
Questo manuale non tratta di RPD in organismi che effettuano operazioni di trattamento che non rientrano nel campo di applicazione del Diritto comunitario, come le agenzie di sicurezza nazionali.

[250] Linee-guida sui RPD del WP29, (nota 239, *supra*) p. 6.

"Autorità o organismo pubblico"

> "Il RGPD non definisce il concetto di 'autorità pubblica o ente pubblico'. Il WP29 è del parere che tale nozione debba essere stabilita dalle normative nazionali. Di conseguenza, il concetto di autorità pubblica o ente pubblico include le autorità nazionali, regionali e locali, anche se, ai sensi del diritto nazionale di applicazione, potrà riguardare un ampio ventaglio di altri organismi di diritto pubblico.[251] Per questi organismi, comunque, la nomina di un RPD è obbligatoria".

Il dovere di nomina del RPD, comunque, si estende oltre questa categoria puramente formale.

Organismi di diritto privato che eseguono "compiti di interesse pubblico" o "esercitano pubblici poteri"

Il WP29 rileva, in riferimento alla specifica base giuridica del trattamento di cui all'Art.6(1)(e) RGPD, che (indipendentemente dalle limitazioni all'obbligo di nomina di un RPD per entità "puramente" private)[252] un RPD dovrebbe sempre essere nominato da titolari del settore privato che eseguono "compiti … nell'interesse pubblico" o che "esercitano un'autorità ufficiale", anche se formalmente non rappresentano "enti pubblici" ai sensi della legislazione nazionale, perché, comunque, in tali attività il loro ruolo è simile a quello delle autorità pubbliche:[253]

> "Un compito di servizio pubblico può essere realizzato, e l'autorità pubblica esercitata non solo da enti e organismi pubblici, ma anche da persone fisiche e giuridiche altre, di diritto pubblico o privato, in settori quali, secondo le disposizioni normative di ciascuno Stato membro, i servizi di trasporto pubblico, la forniture idriche ed energetiche, le forniture stradali, i servizi pubblici di informazione, gli alloggi popolari e gli organismi disciplinari delle professioni regolamentate.
>
> In questi casi, gli interessati possono trovarsi in una situazione molto simile a quella di un trattamento dei loro dati da parte di un'autorità o di un organismo pubblico. In particolare, i dati possono essere trattati per finalità simili e spesso gli interessati non hanno scelta, o hanno solo una scelta limitata, sul come e sul quando i loro dati sono trattati; una situazione di tal genere può richiedere una tutela ulteriore che la nonima di un RPD sarebbe in grado di garantire".
>
> **Anche se non vi è obbligatorietà, il WP29 raccomanda, come buona prassi, che gli organismi privati che svolgono compiti pubblici o esercitano una pubblica autorità nominino un RPD.** Le attività di tale RPD riguardano tutte le operazioni di trattamento svolte, comprese quelle che non hanno a che fare con lo svolgimento di un compito pubblico o l'esercizio di obblighi ufficiali (ed es., la gestione di una banca dati dei dipendenti).

Agli esempi del WP29 si potrebbero aggiungere la gestione, da parte di privati, degli istituti di pena, o di altre istituzioni o servizi statali (come il respingimento di immigrati che risiedono

---

251 Si veda, ad es., la definizione di 'ente pubblico' e 'organismo di diritto pubblico' all'Art. 2(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, GU L 345, 31.12.2003, p. 90 e ss. [nota originale]
Il testo inglese della Direttiva è consultabile su:
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003L0098&from=EN

252 Si veda la nota 248, *supra*.

253 Linee guida sui RPD del WP29 (nota 239, *supra*), p. 6, grassetto aggiunto. L'utilizzo, da parte del WP29, dei termini "compiti di servizio pubblico" e "autorità pubblica" è un mero problema linguistico: nelle linee guida, tali termini si riferiscono a "compiti di pubblico interesse" e "esercizio dell'autorità pubblica" di cui all'Art. 6(1)(e) del RGPD.

illegalmente in un paese). In tutti questi casi, gli organismi privati agiscono come braccio dello Stato – e in tutti questi casi le aziende in questione devono nominare un RPD. Agli Stati membri spetta il compito di chiarire ulteriormente la quastione nelle rispettive legislazioni nazionali e imporre l'obbligo di nomina di un RPD a specifici titolari o tipologie di titolari diversi da quelli delle autorità o degli organismi pubblici deputati (cfr. Art. 37(4)).

ESEMPIO

In **Italia**, l'Autorità nazionale di protezione dei dati, il *Garante,* è del parere che tutti gli organismi o le istanze che ricadano nell'ambito di applicazione degli articoli 18-22 del previgente Codice italiano di protezione dei dati, prevedano l'obbligatorietà di nomina di un RPD. Questi articoli, quindi, stabiliscono le norme generali da applicare al trattamento eseguito da organismi pubblici – quali organismi amministrativi dello Stato, organismi pubblici no-profit a livello nazionale, regionale e locale, autorità locali, università, Camere di commercio, Agenzie di salute pubblica, autorità indipendenti di supervisione, ecc.

Il *Garante* ritiene inoltre che, qualora un organismo privato espleti funzioni di pubblico interesse – sulla base, ad esempio, di una licenza o di una concessione – la nomina di un RPD debba essere caldamente raccomandata, anche se non obbligatoria. Inoltre, in riferimento alle Linee guida sui RPD del WP29, il *Garante* aggiunge che, se un RPD viene nominato su base volontaria, sono di applicazione le stesse norme e condizioni per un RPD nominato su base obbligatoria – e questo a livello dei criteri per la designazione, la posizione e i compiti a lui assegnati.

RPD per i responsabili del trattamento

Come rileva il WP29, l'Articolo del RGPD che impone l'obbligo di designazione di un RPD in determinati casi (Art. 37), come visto in precedenza per il settore pubblico, si applica sia ai titolari che ai responsabili del trattamento.[254] Il testo aggiunge:[255]

> "A seconda di chi soddisfi i criteri sulla designazione obbligatoria, in alcuni casi solo il titolare o solo il responsabile, oppure, in altri casi, sia il titolare che il suo responsabile sono tenuti a nominare un RPD (che avrà il compito di collaborare con entrambi).
>
> E' importante sottolineare che, anche se il titolare soddisfa i criteri di designazione obbligatoria, non è detto che al suo responsabile incomba necessariamente l'obbligo di designazione di un RPD. Questa potrebbe, comunque, costituire una buona prassi".

Nel settore pubblico, visto che per ogni organismo si deve procedere alla designazione di un RPD (come rilevato prima), questo può sembrare un problema di minore importanza. Tuttavia, alla luce dell'ultimo commento del WP29, qualora un'autorità pubblica debba subappaltare attività di trattamento ad organismi privati (come, ad esempio, attività contabili o lo svolgimento di sondaggi) sarebbe quantomeno opportuno scegliere un responsabile che ha designato un RPD, o obbligarne uno, che ancora manca di questa figura, a designarla.

Visto che autorità pubbliche che collaborano insieme possono, a volte, agire da responsabili del trattamento dei dati l'una nei confronti dell'altra, di questa fattispecie dovrebbe

254 Linee-guida sui RPD del WP29 (nota 239, *supra*), sezione 2.2, *DPO del titolare o del responsabile del trattamento*, p. 9.

255 *Idem*. Il WP29 fornisce esempi, tratti dal settore privato, che si incentrano sulle limitazioni all'obbligo di designazione di un RPD per quei settori. Si tratta di esempi non particolarmente utili per questo Manuale.

quantomeno ritrovarsi traccia nei loro accordi scritti, come vedremo nella prossima sottorubrica e nella Terza Parte, sotto-sezione 3.1.

RPD per grandi autorità pubbliche o gruppi di autorità pubbliche

I dati personali sono sempre più oggetto di trattamento in ambiti altamente complessi attraverso complesse architetture tecniche, in cui attori diversi collaborano fra loro e condividono ruoli e relazioni in varie fasi del trattamento anche con riguardo ai rapporti con i cittadini. Questo accade anche nel settore pubblico, che presenta complessità peculiari a livello dei diversi gradi di autonomia di cui possono godere agenzie diverse operanti in un quadro giuridico, amministrativo o costituzionale molto articolato. Come vedremo nella Terza Parte, sezione 3.1, uno dei primi compiti di un neodesignato RPD è quello di analizzare il contesto in cui avviene il trattamento dei dati personali che dovrà controllare e/o su cui sarà chiamato a formulare un parere. Parte del suo compito, infatti, sarà proprio quello di chiarire, in un contesto così complesso, lo statuto dei vari organismi per giungere poi alle opportune disposizioni.

In tal senso va notato che il RGPD sancisce chiaramente (come la Direttiva sulla protezione dei dati del 1995) che "quando le finalità e i mezzi del … trattamento sono determinati dal diritto dell'Unione o degli Stati membri" (come solitamente si verifica per le autorità pubbliche), "il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri" (Art. 4(7)). In tali casi, allora, è sempre opportuno designare un RPD (per tutti i trattamenti previsti da tale fattispecie) presso gli uffici dell'organismo nominato in qualità di titolare del trattamento. La legge (base giuridica) che determina il titolare può sempre, comunque, chiarire questo aspetto.

Se la soluzione non è determinata dalla legge, il problema può essere risolto dal Ministero di governo competente, da un alto funzionario o dagli stessi organismi pubblici a patto che si giunga a chiari accordi in merito a responsabilità e competenze dei vari RPD operanti in istanze diverse all'interno di tale complesso sistema. Tra tali accordi figurano le decisioni sul dove designare uno o più RPD, e i rapporti e le relazioni fra RPD diversi che lavorano in organismi che collaborano operativamente.

Alcuni organismi pubblici molto ampi (o i Ministri di governo o i funzionari di alto rango che vi lavorano) possono decidere di designare più RPD, uno per ciascun organo costitutivo, purché ciò corrisponda all'effettiva attribuzione dei poteri decisionali fra i singoli dipartimenti o le singole unità di tali organismi. Oppure possono designare un solo RPD per tutto l'ente che si interfacci con i responsabili designati di ciascun organo costitutivo; in quest'ultimo caso, come chiarito da un commento del WP29 in materia di designazione dei RPD sulla base di un contratto di servizio (e di cui parleremo nella prossima sottorubrica) ne deriva che questi Responsabili, designati in dipartimenti o settori distinti di grandi organizzazioni, hanno l'obbligo, da un lato, di rispettare le disposizioni in materia di RPD, in particolare quelli relativi ai conflitti di interesse, e, dall'altro lato, di essere tutelati, come il RPD stesso, e non penalizzati nell'esercizio delle loro funzioni di collaborazione con tale figura.[256]

[256] Cfr. Linee guida sui DPO del WP 29 (nota 239, *supra*), sezione 2.4, ultimo trattino, p. 12.

Viceversa, il RGDP permette espressamente a gruppi (formalmente istituiti) di piccoli organismi pubblici – come le autorità locali (in Francia: *communes*) – di decidere (o essere incaricati di) designare congiuntamente un RPD:

> "qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione" (Art. 37(3)).

Questo RPD unico o comune può essere un funzionario di una delle autorità, oppure essere affiancato a un RPD esterno sulla base di un contratto di servizio (come avremo modo di approfondire ulteriormente nella prossima sottorubrica). Se viene designato un DPO centrale (interno e esterno), gli altri (piccoli) organismi possono decidere di nominare, nel proprio organico, un responsabile di collegamento con il RPD centrale – in questo caso valgono, allora, le stesse norme di applicazione per le autorità di dimensioni maggiori: la persona nominata deve rispondere ai requisiti previsti per un RPD e godere delle stesse tutele.

RPD esterni

Come già visto in precedenza, le autorità pubbliche (e le aziende private) non devono creare una posizione interna per un RPD, a meno che non si tratti di una figura a tempo pieno (è probabile che molti organismi più grandi scelgano in tal senso, se non l'hanno già fatto). Infatti:

> "il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizio" (Art. 37(6)).

In Germania, dove la figura del RPD ha visto la luce,[257] studi legali e altri liberi professionisti indipendenti si offrono per ricoprire cariche di RPD. Comunque, anche "associazioni e altri organismi che rappresentano categorie di titolari o responsabili" possono offrire funzioni di RPD ai propri membri in maniera analoga, agendo in nome di tutti (cfr. Art. 37(4)). Si tratta di una fattispecie particolarmente utile alle PMI. Molti gruppi di consulenza e studi legali offrono sostegno e aiuto ai RPD "sulla base di un contratto di servizio", e molte altre imprese più piccole, soprattutto quelle del settore TIC, sono destinate a fare altrettanto secondo le stesse modalità.

Preme sottolineare che questi RPD esterni, comunque, non devono essere troppo estranei all'ambiente per cui lavorano: come chiariremo nella prossima parte del Manuale, i RPD devono avere una piena e profonda comprensione degli organismi per i quali prestano la loro opera e delle attività di trattamento. Devono inoltre essere pienamente e facilmente raggiungibili – dal personale degli organismi in questione, dai soggetti interessati e dalle autorità di protezione dei dati (autorità di supervisione). I loro dati di contatto devono chiaramente figurare nei siti web delle rispettive autorità, nei pieghevoli e nel materiale informativo ecc.

L'autorità francese della protezione dei dati, la CNIL, ritiene che un RPD debba, "di preferenza", essere un membro del personale dell'organizzazione del titolare, ma ammette che, per le PMI, questo non sempre possa essere possibile.[258]

---

257 Si veda la sotto-sezione 2.3.1, *supra*.

258 CNIL, *Guide Pratique Correspondant* (nota 246, *supra*), p. 6.

Nel settore pubblico, è spesso preferibile che il RPD provenga da un particolare settore interessato; per esempio, come visto nella precedente sottorubrica, è meglio un RPD di provenienza da un grosso organismo pubblico o un RPD esterno per un gruppo di autorità più piccole – piuttosto che uno proveniente da uno studio privato con il ruolo di RPD esterno, anche se questo dipende sempre, alla fin fine, dalla cultura e dalle prassi del paese in questione.

2.5.3 Qualifiche, competenze e posizione del RPD

Competenze professionali richieste

Il Regolamento sancisce che:

> "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" [come vedremo al punto 2.3.4, *infra*].
>
> (Art. 37(5), grassetto aggiunto).

Sul primo punto, – la conoscenza specialistica –, il Documento istituzionale dell'UE sugli "standard professionali" dei RPD rileva le seguenti necessità:[259]

> (a) conoscenza specialistica in materia di privacy e legislazione sulla protezione dei dati nell'UE, in particolare dell'Art. 16 del Trattato relativo al funzionamento dell'Unione Europea, dell'Art. 8 della Carta dei Diritti Fondamentali dell'Unione Europea, del Regolamento (CE) 45/2001 e degli altri rilevanti strumenti giuridici di protezione dei dati e conoscenze in materia di IT e sicurezza IT; inoltre
>
> (b) buona conoscenza del funzionamento dell'istituzione [in cui il RPD viene designato], delle attività di trattamento dei dati da essa operate e abilità interpretativa delle norme relative alla protezione dei dati in tale contesto.

La conoscenza tecnica dei sistemi di IT viene particolarmente sottolineata. Come afferma l'Autorità **francese** di protezione dei dati, la CNIL:[260]

> "Per quanto riguarda l'informatica, si richiede una buona comprensione della terminologia, delle attività [IT] e delle diverse forme di trattamento dei dati. Un RPD deve possedere, ad esempio, conoscenze in materia di gestione dei dati e sistemi di utilizzo degli stessi, tipologie di software, sistemi di stoccaggio dei dati e dei file, normative in materia di riservatezza e politiche di sicurezza (cifratura dei dati, firma elettronica, dati biometrici, …). Tali conoscenze devono permettere [al RPD] di controllare la realizzazione dei progetti IT e fornire utili pareri al titolare responsabile del trattamento".

Anche il Considerando 97 del RGPD sottolinea che:

> "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".

---

259 Rete dei RPD delle Istituzioni e degli Organismi dell'UE, Qualifiche professionali per i RPD delle Istituzioni e degli Organismi dell'UE che lavorano ai sensi del Regolamento (CE) 45/2001 (nota 241, *supra*), pp. 3 – 4.

260 CNIL, *Guide Pratique Correspondant* (nota 246, *supra*), p. 8 (traduzione nostra).

In altri termini, la natura delle "competenze tecniche" e delle "capacità" può variare a seconda delle attività del titolare: un RPD che lavora per il fisco avrà bisogno di competenze diverse da un RPD che lavora nell'istruzione o nel campo della previdenza sociale. Il GEPD parla del bisogno di "**prossimità**" (fra il RPD e l'organismo per il quale lavora):[261]

> "Il DPO ricopre un ruolo centrale presso la sua istituzione/organismo: i RPD conoscono [cioè devono conoscere] i problemi degli organismi presso cui lavorano (*idea di prossimità*) e, alla luce del loro status, giocano un ruolo chiave nel formulare pareri e nel cercare di risolvere i problemi in materia di protezione dei dati [di quello specifico organismo]".

Come affermano le Linee guida sui RPD del WP29:[262]

> "Il RPD deve dimostrare una buona comprensione delle attività di trattamento svolte [nel settore o nell'organizzazione di appartenenza], dei sistemi di informazione, dei sistemi di protezione dei dati, e delle necessità di tutela dei dati del titolare.
>
> Nel caso di autorità o organismo pubblico, il RPD deve possedere solide conoscenze delle procedure e delle regole amministrative [interne] dell'organizzazione".

E, possiamo aggiungere: della giurisprudenza, della normativa e delle procedure che regolamentano gli organismi pubblici di riferimento (ad es., Diritto tributario, Diritto allo studio ecc.), del Diritto amministrativo e delle procedure in generale.

Dall'altro canto, come viene fatto notare alla rubrica "*Conflitti di interesse*" e "*Posizione interna all'organizzazione*", la designazione di un appartenente al personale di un organismo pubblico può causare problemi, soprattutto se il Responsabile fosse nominato part-time e continuasse a ricoprire altre cariche nell'organismo in questione.

Le competenze tecniche in materia di normativa e pratica della protezione dei dati possono essere comprovate con corsi di formazione, corsi on e off-line frequentati dalla persona in questione – come quelli offerti dal Programma "T4DATA" di cui fa parte questo Manuale -ma l'offerta formativa, sia a livello di quantità che di qualità e varieta, è molto ampia, come torneremo a sottolineare.

Formazione ufficiale e certificazione

Al momento della stesura di questo testo (dicembre 2018), solo la Spagna, fra gli Stati membri dell'UE, aveva avviato la creazione di un sistema formale di certificazione destinato ai RPD (peraltro a tutt'oggi non operativo).[263] Inoltre, questo schema di certificazione dei RPD (e altri in via di definizione) si fondano sulla norma ISO 17024, ossia su una norma che disciplina gli

---

[261] GEPD, Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001 (nota 240, *supra*), p. 5, grassetto aggiunto.

[262] Linee guida sui DPO del WP29 (nota 239, *supra*), p. 11.

[263] L'Autorità nazionale spagnola sulla protezione dei dati, la *Agencia Española de Protección de Datos* (AEPD) ha creato un sistema di certificazione per i DPO (*Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos – Esquema AEPD-DPD*) sotto l'ombrello dell'Agenzia nazionale spagnola di accreditamento (*la Entidad Nacional de Acreditación – ENAC*) che può convalidare gli organismi di certificazione (*Entidades de Certificación*), i quali poi rilasciano i pertinenti riconoscimenti sulla base dei criteri fissti dalla DPA (AEDP) e di un esame ufficiale, si veda:
https://www.aepd.es/reglamento/cumplimiento/common/esquema-aepd-dpd.pdf (versione 1.3, 13 giugno 2018).
Finora, nessun organismo di certificazione è stato accreditato e nessuna cerificazione RPD rilasciata.
Si veda anche la breve discussione, più generale, sui sistemi di certificazione al punto 2.1, *supra*.

schemi di certificazione riservati a persone fisiche e professionisti. Da questo punto di vista, gli schemi in oggetto non soddisfano i requisiti della norma ISO 17065 cui fa riferimento la disposizione sulla certificazione contenuta nel RGPD, riferita, appunto alla certificazione di servizi, prodotti, ed eventualmente di sistemi gestionali. Ne deriva che le certificazioni dei RPD, pur lodevoli in sé, sono diverse dalle "certificazioni" a norma dell'Art. 42 del RGPD.

In Francia sono stati pubblicati dalla CNIL due "referentiels", ossia due specifiche di riferimento, relative a certificazioni dei RPD (11 ottobre 2018). Una riguarda la certificazione delle competenze dei RPD, e l'altra la previsione delle competenze richieste ai RPD e agli organismi di accreditamento autorizzati a certificare RPD.[264]

In Germania, l'offerta di corsi e seminari di formazione è molto alta e, in alcuni casi, certificata,[265] ma, nonostante si tratti di una lunga e consacrata tradizione, non esistono percorsi formativi obbligatori per legge o sistemi ufficialmente riconosciuti. Molte delle associazioni nazionali e internazionali di RPD, che abbiamo visto prima, offrono formazione a livello specialistico, – ma, ancora una volta, nulla di obbligatorio.[266]

Molti di questi corsi e seminari di formazione sono finalizzati ad offrire ai partecipanti conoscenze specialistiche sul RGPD e sui compiti affidati al RPD ai sensi del RGPD. Il RGPD, peraltro, (come il diritto tedesco e quello di altri paesi) non stabilisce specificamente criteri dettagliati di formazione o sistemi di certificazione. È probabile che in futuro, sull'esempio della Spagna, anche altri Stati membri organizzino sistemi formali e ufficialmente riconosciuti e/o che il Comitato europeo per la protezione dei dati ne approvi alcuni (presumibilmente su una base informale).[267] Fino a quel momento, però, la situazione rimane piuttosto fluida. Come ben sottolinea l'Autorità **italiana** della protezione dei dati, il *Garante*:[268]

> "Come accade nei settori delle cosiddette "professioni non regolamentate", si sono diffusi schemi proprietari di certificazione volontaria delle competenze professionali effettuate da appositi enti certificatori. Tali certificazioni (che non rientrano tra quelle disciplinate dall'art. 42 del RGPD) sono rilasciate anche all'esito della partecipazione ad attività formative e al controllo dell'apprendimento.
>
> Esse, pur rappresentando, al pari di altri titoli, un valido strumento ai fini della verifica del possesso di un livello minimo di conoscenza della disciplina, tuttavia non equivalgono, di per sé, a una "abilitazione" allo svolgimento del ruolo del RPD né, allo stato, sono idonee a sostituire

---

[264] Si veda https://www.cnil.fr/fr/certification-des-competences-du-dpo-la-cnil-adopte-deux-referentiels

[265] Cfr, ad es.: https://www.datenschutzexperten.de/grundlagenseminar-ausbildung-betrieblicher-datenschutzbeauftragter-nach-bdsg-mit-dekra.html

[266] Il documento istituzionale dell'UE sulle qualifiche per i RPD raccomanda i sistemi della International Association of Privacy Professionals (IAPP). La IAPP offre certificazioni specifiche per regione, compresa una dedicata all'Europa orientale che copre anche la formazione in materia di RGPD. Si veda: https://iapp.org/certify/cippe/
Rete dei RPD delle Istituzioni e degli Organismi dell'UE, Standard Professionali per i RPD delle Istituzioni e degli Organismi dell'UE che lavorano ai sensi del Regolamento (CE) 45/2001 (nota 241, *supra*), p. 5.
Il documento istituzionale dell'UE sui RPD parla anche di gestione della sicurezza IT e di certificazione di audit, ma si tratta di questioni più generali e non specificamente finalizzate alla protezione dei dati.

[267] Le Linee guida sui RPD del WP29 (nota 239, *supra*) affermano semplicemente che "la promozione e l'adeguata e regolare formazione dei RPD da parte delle autorità di supervisione può costituire un elemento utile." (p. 11).

[268] *Garante della Privacy*, FAQ sui RPD (nota 246, *supra*), sezione 3.

> il giudizio rimesso alle PP.AA. nella valutazione dei requisiti necessari al RPD per svolgere i compiti previsti dall'art. 39 del RGPD.**(3)**".

Come afferma la Confederazione delle Organizzazioni europee sulla protezione dei dati (CEDPO):[269]

> "Per mostrarvi quanto siano qualificati, i candidati probabilmente snocciolerannno diplomi e certificati accumulati negli anni. Ma come valutare un CV di valore da uno di scarso peso? Primo, valutando le credenziali dell'organismo di formazione e di certificazione. Se si tratta di una ben nota ed accreditata organizzazione nazionale o pan-europea (in alcuni paesi anche le Autorità di protezione dei dati sono organismi di certificazione), potete già stare più tranquilli. E poi, guardate con quale frequenza i corsi di formazione sono stati seguiti. Una singola giornata, un certificato ottenuto a pagamento o un esame pro-forma non possono garantire la formazione di nessun RPD degno di questo nome".

Tutti i vari documenti di orientamento sottolineano la necessità, per le organizzazioni, di garantire che i loro RPD continuino a mantenere e migliorare le loro competenze tecniche, anche dopo la designazione, partecipando a corsi e seminari specializzati, come del resto stabilito dal RGPD (si veda l'ultimo enunciato all'Art. 38(2)). Come afferma il WP29:[270]

> "I RPD devono usufruire della possibilità di rimanere aggiornati sugli sviluppi che riguardano la protezione dei dati. Lo scopo deve essere quello di aumentare costantemente il livello delle conoscenze tecniche dei RPD incoraggiandoli a partecipare a corsi di formazione sulla protezione dei dati e altre forme di sviluppo professionale con la partecipazioni a convegni sulla privacy, gruppi di lavoro, ecc".

L'Autorità **francese** sulla protezione dei dati, la CNIL, ha creato uno speciale (e molto utile) "**extranet**" per RPD registrati, accessibile solamente su autenticazione, che mette a disposizione testi normativi (leggi, decreti, ecc.), segnala opportunità di formazione e di informazione, compresi i rapporti e i testi di orientamento elaborati dalla CNIL, e altri supporti pratici e giuridici, offrendo così agli interessati un forum di discussione e di scambio di punti di vista.[271]

Esperienza

Le Linee guida sui RPD del WP29 non parlano del problema dell'esperienza che un RPD dovrebbe aver accumulato. La Rete dei RPD istituzionali dell'UE, comunque, raccomanda che abbiamo maturato almeno:[272]

> "almeno 3 anni di esperienza lavorativa [vedi *infra*] come RPD in un organismo in cui la protezione dei dati non rappresenti l'attività principale [*idem*]" (e in cui le attività di trattamento dei dati personali siano prevalentemente di carattere amministrativo); e
>
> "almeno 7 anni di esperienza lavorativa come RPD in un'istituzione dell'UE o in un'organismo dell'UE in cui la protezione dei dati personali costituisce l'attività

---

269 CEDPO, Choosing the best candidate as your Data Protection Officer (DPO) – Practical guidelines for organisations (nota 236, *supra*), p. 2.

270 Linee guida sui RPD del WP29 (nota 239, *supra*), p. 14.

271 CNIL, *Guide Pratique Correspondant* (nota 246, *supra*), sezione 4.

272 Rete dei RPD delle Istituzioni e degli Organismi dell'UE, Qualifiche professionali per i RPD delle Istituzioni e degli Organismi dell'UE che lavorano ai sensi del Regolamento (CE) 45/2001 (nota 241, *supra*), p. 4.

> principale o che gestisce un volume importante di operazioni di trattamento dei dati personali".

Una nota aggiunge che:

> "L'esperienza acquisita include esperienza sull'attuazione dei requisiti in materia di protezione dei dati e sul funzionamento della istituzione/organizzazione designante. In assenza degli anni di esperienza richiesti, l'istituzione/organizzazione designante deve offrire più tempo al RPD per attività di formazione e attività operative nel settore della protezione dei dati".

Per quanto riguarda il problema che il trattamento dei dati personali costituisca "l'attività principale" dell'organizzazione interessata, questo concetto (che ritroviamo anche nel RGPD ove si parla delle "attività principali del titolare o del responsabile") viene chiarito dalle Linee-guida del WP29:[273]

> "Attività principali" ('Core activities') possono essere considerate le operazioni chiave necessarie al raggiungimento delle finalità del titolare o del responsabile".

Il concetto di "esperienza acquisita" non deve specificamente essere interpretato come esperienza specialistica – può trattarsi dell'esperienza nell'elaborazione e nell'attuazione di politiche in quella determinata organizzazione (o in altra simile), dell'esperienza in aree rilevanti come IT, sviluppo di prodotti, ecc. ... Basti rilevare che la posizione non può essere assegnata a una persona troppo giovane e con scarsa esperienza o a una persona che non conosce il tipo di organizzazione in cui lavora.

Caratteristiche e qualità personali

Il GEPD, la Rete istituzionale dell'UE sui RPD e il CEDPO fanno tutti giustamente notare che un RPD deve avere qualità personali particolari. E' una figura che si trova in una posizione delicata, che deve saper dire "no" ai superiori, anche se in rari casi, ed essere capace di mediare e risolvere i problemi in maniera accettabile per l'organizzazione, ma nel pieno rispetto della legge (e del rafforzamento della privacy). Come affermano le Linee guida del WP29:[274]

> "Le qualità personali devono includere, ad esempio, l'integrità ed un'elevata etica professionale; l'interesse primario del RPD deve essere quello di garantire la conformità al RGPD. Il RPD ha un ruolo chiave nel promuovere la cultura della protezione dei dati nell'organizzazione in cui lavora e nel coadiuvare l'applicazione degli elementi essenziali del RGPD …

La Rete dei RPD delle istituzioni dell'UE sottolinea l'importanza delle seguenti qualità "personali" e "relazionali":[275]

> "Qualità personali: integrità, iniziativa, organizzazione, tenacia, discrezione, capacità di affermarsi in circostanze difficili, interesse nella protezione dei dati e motivazione a diventare un RPD.

---

273 Linee guida sui RPD del WP29 (nota 239, *supra*), p. 6.

274 Linee guida sui RPD del WP29 (nota 239, *supra*), p. 11.

275 Rete dei RPD delle Istituzioni e degli Organismi dell'UE, Qualifiche professionali per i RPD delle Istituzioni e degli Organismi dell'UE che lavorano ai sensi del Regolamento (CE) 45/2001 (nota 241, *supra*), p. 4.

> Qualità relazionali: capacità di comunicazione, capacità negoziali, capacità di risoluzione delle controversie, capacità relazionali sul luogo di lavoro".

In un altro punto si sottolinea:[276]

> "La natura stessa dei compiti del RPD spesso richiede un atteggiamento deciso e tenace anche verso quei titolari che ricoprono posizioni di alto livello, attitudine che potrebbe essere interpretata, nella migliore delle ipotesi, come formalistica oppure, nel peggiore dei casi, come "provocatoria". Il RPD deve, quindi, essere in grado di sostenere le pressioni e affrontare le difficoltà inerenti ad una posizione così importante".

Il CEDPO aggiunge:[277]

> "Il RPD deve affrontare un gran numero di sfide e compiti molto diversi. Per questo deve dare prova di abili competenze comunicative associate ad una raffinata capacità diplomatica. Un RPD non è (e non deve essere) un "attivista della privacy": coadiuvato dagli altri leader dell'organizzazione, deve farsi carico del ruolo di responsabile dello sviluppo operativo e aiutare la sua organizzazione ad includere la privacy nel processo decisionale, non solo individuando e prevenendo i rischi, ma anche creando valore aggiunto. Inoltre, il RGPD stabilisce che il RPD si interfacci con il livello gerarchico più alto e che la sua indipendenza sia garantita. Questo richiede sia "serietà" che capacità di leadership".

Indipendenza

Abbiamo già rilevato che "il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi" (Art. 37(6)). Si tratta, comunque, di una posizione che non è mai quella di un semplice impiegato o di un funzionario. In particolare, il Regolamento sancisce che:

> "Tali responsabili della protezione dei dati, dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro assegnati in maniera indipendente" (Considerando 97).

Nello specifico, il Regolamento stabilisce:

> "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".
>
> (Articolo 38(3))

Il WP29 chiarisce il concetto nel modo seguente:[278]

> "[tale disposizione] significa che [], nell'adempiere ai compiti di cui all'Articolo 39, i RPD non devono ricevere istruzioni, ad esempio, su come affrontare un problema, quali

---

276 *Idem*, p. 6. La Rete raccomanda di alleggerire tali pressioni nel contesto della discussione sulla posizione da accordare al RPD nella sua organizzazione, come visto alla rubrica "*Posizione del RPD all'interno della sua organizzazione*", *infra*.

277 CEDPO, Choosing the best candidate as your Data Protection Officer (DPO) – Practical guidelines for organisations (nota 236, *supra*), p. 3 (solo lievi modifiche).

278 Linee guida sui RPD del WP29 (nota 239, *supra*), sezione 3.3, pp. 14 – 15.

> risultati raggiungere, come dare seguito ad una denuncia o se consultare o meno l'autorità di controllo. Inoltre, non devono ricevere orientamenti sul punto di vista da adottare per trattare problemi normativi sulla protezione dei dati o seguire una particolare interpretazione giurisprudenziale.
>
> L'autonomia dei RPD, peraltro, non significa che godano di poteri decisionali al di là dei compiti stabiliti per loro all'Articolo 39.
>
> Il titolare o il responsabile rimangono i responsabili della conformità alle normative sulla protezione dei dati e devono poterla garantire. Se il titolare o il responsabile prendono decisioni incompatibili con il RGPD e con i pareri del RPD, egli deve avere la possibilità di formulare un chiaro dissenso ai responsabili di tali decisioni".

Come vedremo nella Terza Parte, il parere del RPD – e ogni azione intrapresa contro questo parere – devono essere registrati e possono essere utilizzati contro il titolare o il responsabile in caso di indagine da parte delle relative autorità di protezione dei dati (come già visto, al contrario, il fatto che un titolare o un responsabile agiscano in accordo con il parere o gli orientamenti del RPD può essere considerato un "elemento" per la dimostrazione della conformità al RGPD (Considerando 77).[279]

Anche il WP29 chiarisce la portata della disposizione secondo cui il RPD "non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti":[280]

> "Si tratta di una norma che rafforza l'autonomia del RPD, ne garantisce l'azione indipendente e la necessaria e sufficiente tutela nell'adempimento dei compiti relativi alla protezione dei dati.
>
> Il RGPD proibisce sanzioni solo nel caso in cui siano imposte come conseguenza dell'adempimento dei compiti del RPD nell'esercizio delle sue funzioni. Per esempio, un RPD valuta che un particolare trattamento dei dati possa generare un rischio elevato e chiede al titolare o al responsabile di procedere con una valutazione di impatto sulla protezione dei dati, ma sia il titolare che il responsabile non sono d'accordo con questa richiesta. In una simile fattispecie, il RPD non può essere rimosso o penalizzato per aver espresso la sua opinione.
>
> Le sanzioni possono avere molte forme e carattere sia diretto che indiretto. Possono consistere, ed esempio, in un'assenza o un ritardo di promozioni; ostacoli all'avanzamento di carriera; negazione di benefit che altri collaboratori ricevono. Non è necessario che tali sanzioni si concretizzino, basta che siano minacciate e siano utilizzate per penalizzare il RPD nell'ambito delle sue attività.
>
> Come normale regola di gestione, e come avverrebbe per qualunque lavoratore o contraente nel quadro di un contratto nazionale di lavoro o del diritto penale, un RPD può essere oggetto di legittimo licenziamento per motivi non attinenti all'esecuzione di compiti o mansioni che gli sono propri (ad esempio, in caso di furto, molestie fisiche, psicologiche o sessuali o colpa grave).
>
> In questo contesto va rilevato che il RGPD non specifica come e quando il RPD debba essere licenziato o sostituito. In ogni caso, più il contratto di lavoro di un RPD è stabile e agganciato ad un quadro normativo solido, maggiori saranno le garanzie contro i

279 Si veda la sezione 2.2.2, *supra*.

280 Linee guida sui RPD del WP29 (nota 239, *supra*), sezione 3.4, p. 15.

> licenziamenti abusivi, maggiore l'indipendenza d'azione del RPD. Per questi motivi, il WP29 accoglie con favore gli sforzi delle organizzazioni in tale direzione".

Il contratto di lavoro offerto ad un RPD dovrebbe, quantomeno, includere, clausole sull'indipendenza che riprendano il dettato del RGPD, oppure aperti riferimenti a questi dispositivi. Tribunali e corti giudicanti su casi di questo genere devono, inoltre, tener conto, senza eccezioni, delle norme del RGPD in materia. Qualora necessario, anche il diritto del lavoro deve essere modificato a tal fine e gli Stati membri devono sostenere l'indipendenza dei RPD nelle legislazioni nazionali: esempi di garanzie contro il licenziamento di figure assimilabili si possono ritrovare, ad esempio, nelle norme che tutelano i responsabili sindacali e/o che richiedono l'approvazione dei comitati dei lavoratori per la nomina o il licenziamento da certe funzioni.

NB: il Gruppo istituzionale dell'UE sui RPD affronta il problema dell'indipendenza e dei conflitti di interesse (il prossimo argomento che tratteremo anche noi in questo Manuale), soprattutto in termini di durata contrattuale della nomina e altre garanzie (si veda la rubrica "*Posizione del RPD all'interno della sua organizzaione*", *infra*). Il CEDPO si limita a notare che l'organizzazione che nomina il RPD deve "valutare … come tutelare l'indipendenza del RPD".[281]

Conflitto di interessi

Come fa notare il WP29:[282]

> "L'Articolo 38(6) prevede che il RPD possa 'svolgere altri compiti e funzioni', ma richiede, comunque, che l'organizzazione si assicuri che 'tali compiti e funzioni non diano adito ad un conflitto di interessi'.
>
> L'assenza di un conflitto di interessi è strettamente legata all'obbligo di operare in maniera indipendente. Sebbene i RPD possano svolgere altri compiti e funzioni, si tratta sempre di mansioni che non possono generare in alcun modo un conflitto di interessi. Questo determina, in particolare, che il RPD non possa ricoprire nell'organizzazione una posizione che gli permetta di stabilire mezzi e finalità del trattamento dei dati personali. Alla luce della specifica struttura organizzativa di ciascuna organizzazione sarà necessaria una disanima caso per caso.
>
> In linea di massima, si possono considerare posizioni conflittuali funzioni direttive (come quelle di amministratore delegato, direttore generale, direttore finanziario, direttore sanitario, responsabile del dipartimento marketing, responsabile risorse umane o responsabile del dipartimento IT), ma anche ruoli gerarchici più bassi della struttura organizzativa se tali ruoli o funzioni generano un impatto sui mezzi e le finalità del trattamento.
>
> A seconda delle attività, delle dimensioni e della struttura dell'organizzazione, rappresenta una buona pratica per titolari e responsabili:
>
> - identificare le funzioni incompatibili con quelle di RPD;
> - elaborare regole interne per evitare il conflitto di interessi;
> - elaborare spiegazioni più generali sul conflitto di interessi;
> - dichiarare che il proprio RPD non è in situazione di conflitto di interessi con la sua funzione, e questo come strategia di sensibilizzazione su tale requisito;

---

281 CEDPO, Choosing the best candidate as your Data Protection Officer (DPO) – Practical guidelines for organisations (nota 236, *supra*), p. 3.

282 Linee guida sui RPD del WP29 (nota 239, *supra*), sezioni 3.5, pp. 15 – 16. Il terzo paragrafo ("In linea di massima …") è in nota al documento, e non nel *corpus* del testo, come qui.

- includere garanzie negli statuti interni dell'organizzazione e assicurare che l'avviso di posto vacante per la funzione di RPD o il contratto di servizio siano sufficientemente precisi e dettagliati da evitare un conflitto di interessi. In tale contesto va tenuto presente che il conflitto di interesse può assumere varie forme, a seconda che il RPD sia assunto in interno o all'esterno.

Il Gruppo istituzionale dell'UE sui RPD aggiunge:[283]

> Il RPD non deve trovarsi in una situazione di conflitto di interessi fra le sue funzioni come RPD e altre funzioni ufficiali, in particolare quelle legate all'applicazione dei dispositivi del Regolamento (Art. 24.3). Il conflitto di interesse si origina laddove gli altri compiti che si richiede ad un RPD di assolvere possono direttamente generare interessi avversi a quelli della protezione dei dati personali in seno all'organizzazione cui il RPD appartiene. Se del caso, egli deve avere facoltà di sollevare il problema con l'autorità che lo ha nominato.

Come vedremo nel prossimo punto, il Gruppo tratta il problema in modo più dettagliato a livello della durata della nomina e di altre garanzie. Il CEDPO ancora una volta si limita a notare che, se la nomina del RPD non riguarda un'occupazione full-time, l'organizzazione che lo impiega ha l'obbligo "di valutare … come gestire il conflitto di interessi".[284]

Posizione del RPD in seno all'organizzazione

La posizione gerarchica e contrattuale del RPD in seno alla sua organizzazione è di fondamentale importanza per garantirne l'efficacia, l'indipendenza e la mancanza di conflitto di interessi.

Da un lato, come già detto, il RPD deve essere "vicino" all'organizzazione nella quale presta servizio (si veda *supra*, alla rubrica "*Esperienza richiesta*"). Inoltre, come il CEDPO sottolinea:[285]

> "affinchè il RPD sia efficace, deve essere presente e sul terreno, non solo disponibile nei confronti delle parti interessate dell'organizzazione, ma anche attivamente alla ricerca di opportunità per interagire con i diversi dipartimenti".

Questo può essere un problema nel caso in cui il RPD provenga dall'esterno e abbia un contratto di servizio perchè, per definizione, non fa parte dell'organismo cui presta i suoi servigi. Nel settore privato, e in alcuni paesi come la Germania, ci sono sicuramente RPD esterni che hanno maturato una lunga esperienza nel settore o sotto-settore in cui lavorano. Nel settore pubblico, la situazione può essere più complicata (v. sezione 2.3.2, *supra* alla rubrica "*RPD per grandi autorità pubbliche o gruppi di autorità pubbliche*" e "*RPD esterni*").

Esiste comunque sempre una tensione fra, da un lato, la necessaria "vicinanza" del RPD alla sua organizzazione, e, dall'altro, la necessità di evitare il conflitto di interessi e tutelare, nel concreto, l'indipendenza d'azione del RPD.

Come già osservato, nel parere del WP29 questo significa che il RPD non può essere coinvolto nello stabilire mezzi e finalità del trattamento dei dati personali e non può ricoprire posizioni

---

283 Rete dei RPD delle Istituzioni e degli Organismi dell'UE, Standard Professionali per i RPD delle Istituzioni e degli Organismi dell'UE che lavorano ai sensi del Regolamento (CE) 45/2001 (nota 241, *supra*), p. 15.

284 CEDPO, Choosing the best candidate as your Data Protection Officer (DPO) – Practical guidelines for organisations (nota 236, *supra*), p. 3.

285 *Idem*, p. 2.

di alta dirigenza quali la carica di amministratore delegato, o responsabile di un grosso dipartimento.[286]

Il problema è trattato più nel dettaglio dal Gruppo istituzionale dell'UE sui DPO e, sebbene la sua posizione debba essere analizzata alla luce dello specifico contesto, è comunque utile ricordarla. Dopo aver rilevato le molte disposizioni del Regolamento che trattano del tema (Regolamento (CE) 45/2001)[287] e sono finalizzate a garantire l'indipendenza di questa figura, il Gruppo afferma:[288]

> "nella pratica, comunque, potrebbe non avverarsi semplice, per un RPD, esercitare le proprie funzioni in modo pienamente indipendente. E' inutile ribadire che la situazione individuale e la personalità del RPD hanno la loro importanza, ma è innegabile che ci siano degli elementi che tendano ad indebolirne la posizione:
>
> - un RPD part-time vive un conflitto permanente fra il consacrare sforzi e tempo alle sue funzioni di RPD e alle funzioni in un altro ambito. Per quanto riguarda gli sviluppi di carriera e gli obiettivi raggiunti, l'organizzazione potrebbe attribuire un gran peso alle attività non legate ai compiti di RPD, e questo potrebbe ingenerare pressioni affinchè il RPD si concentri su mansioni non legate a questa carica. Un RPD a tempo parziale corre anche il rischio di ritrovarsi in una situazione di conflitto di interessi;
> - un RPD con un contratto a termine è in una posizione più debole nell'espletamento delle sue funzioni rispetto a un RPD con un contratto a tempo indeterminato (funzionario o agente temporaneo con un contratto di lavoro a tempo indeterminato). Il timore potrebbe essere quello che l'espletamento delle proprie funzioni possa avere un impatto negativo sul rinnovo contrattuale. Un RPD giovane e con scarsa esperienza può essere in difficoltà nell'affrontare i titolari del trattamento ed essere più preoccupato dei propri sviluppi di carriera che dell'investirsi nelle sue funzioni di RPD;
> - un RPD che riporta a, ed è valutato da, un diretto superiore (direttore o capo-unità) gerarchico, può sentirsi spinto a fare gioco di squadra e per questo a non contrastare colleghi e superiori, magari pensando che un'attitudine più intransigente per quanto riguarda i compiti legati alle funzioni di RPD possano avere un impatto negativo sulla sua carriera. ... Per evitare tali pressioni, il RPD deve far relazione a ed essere valutato dal superiore amministrativo della sua

---

286 Si veda *supra*, alla rubrica "*Conflitto di interessi*", in particolare il terzo paragrafo dalle Linee guida sui DPO del WP29. L'autorità italiana sulla protezione dei dati, il *Garante*, nelle sue FAQ sul RPD, afferma invece:

> … In merito, l'art. 38, par. 3, del RGPD stabilisce che il RPD «riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento». Tale rapporto diretto garantisce, in particolare, che il vertice amministrativo venga a conoscenza delle indicazioni e delle raccomandazioni fornite dal RPD nell'esercizio delle funzioni di informazione e consulenza a favore del titolare o del responsabile.
>
> Alla luce delle considerazioni di cui sopra, nel caso in cui si opti per un RPD interno, sarebbe quindi in linea di massima preferibile che, ove la struttura organizzativa lo consenta e tenendo conto della complessità dei trattamenti, la designazione sia conferita a un dirigente ovvero a un funzionario di alta professionalità, che possa svolgere le proprie funzioni in autonomia e indipendenza, nonché in collaborazione diretta con il vertice dell'organizzazione (*Garante*, Faq sul RPD [nota 213, *supra*], sezione 2.)

Forse il modo migliore per riconciliare le posizioni del WP29 e del *Garante* a tale proposito, sarebbe di suggerire che il RPD sia nominato *al livello di* un capo dipartimento o un alto dirigente, ma senza essere responsabile delle operazioni di trattamento dei dati.

287 Si veda la nota 241, *supra*.

288 Rete dei RPD delle Istituzioni e degli Organismi dell'UE, Standard Professionali per i RPD delle Istituzioni e degli Organismi dell'UE che lavorano ai sensi del Regolamento (CE) 45/2001 (nota 241, *supra*), pp. 6 – 7.

organizzazione. Questo aspetto è di particolare rilevanza per i RPD part-time, che riportano a e sono valutati dall'autorità che li nomina e/o dal diretto superiore gerarchico;

- un RPD che ha la necessità di richiedere personale e risorse (risorse IT, un bilancio per viaggi e formazioni) al suo diretto superiore gerarchico può essere in difficoltà se costui non è pienamente coinvolto nel raggiungimento della conformità della protezione dei dati. La situazione può essere evitata se il RPD gestisce un proprio budget e può richiedere l'approvazione di risorse aggiuntive all'autorità che lo ha nominato.

Buone regole che aiutano a garantire l'indipendenza del RPD sono le seguenti:

- l'ente o l'organismo deve creare la posizione interna di RPD a livello di Consulente, Capo unità o Direttore e, nel caso in cui la posizione sia ufficialmente riconosciuta come di livello manageriale, questa deve figurare nell'organigramma ufficiale dell'ente/dell'organismo in questione;
- l'ente o l'organismo deve nominare il RPD per il periodo più lungo possibile, in linea con il contratto dello stesso. Un periodo di cinque anni dovrebbe, pertanto, costituire la norma, a meno di condizioni diverse;
- il RPD deve firmare con l'ente o l'organismo un contratto a tempo indeterminato/permanente e deve possedere un'esperienza adeguata(…);
- il RPD deve essere in grado di dedicarsi a tempo pieno alle sue funzioni di RPD, soprattutto nel caso di grandi enti o istituzioni; per quanto riguarda organismi più piccoli, deve consacrare tutto il tempo necessario almeno alla fase di avviamento del regime di protezione dei dati. E' obbligatorio che gli vengano fornite risorse e *infra*strutture. Le mansioni di un RPD part-time che esulano da quelle di RPD, non devono generare conflitto di interessi, reale o apparente, con i compiti di RPD;
- le organizzazioni in cui opera un RPD e in cui le attività di trattamento dei dati costituiscono l'attività principale, e per questo necessitano di molto personale, devono garantire tale capacità in risorse umane;
- le organizzazioni devono prevedere norme che garantiscano la collaborazione fra il proprio personale e il RPD senza ordini o permessi espliciti dei superiori gerarchici;
- il RPD riporta al capo dell'ente o dell'organismo responsabile della valutazione dei risultati del RPD nell'espletamento delle proprie funzioni, come previsto dal Regolamento. Il responsabile della valutazione dei risultati del RPD deve essere consapevole che il Responsabile debba anche prendere posizioni non sempre apprezzate dall'organizzazione. Il RPD non deve subire conseguenze di valutazione per l'espletamento delle proprie funzioni. L'organismo che ha il potere di nomina deve garantire che durante il mandato del RPD egli possa beneficiare almeno dei "normali" avanzamenti di carriera. Nella valutazione dei risultati del RPD, il valutatore sarà attento a non esprimere biasimo per eventuali posizioni impopolari difese dal RPD né a considerare le norme di protezione dei dati come oneri amministrativi. Per un RPD part-time, la valutazione dei compiti legati alle sue funzioni come RPD deve essere pari a quella di altri compiti eseguiti al di fuori di tali funzioni … ;
- il RPD deve avere a disposizione una propria linea di bilancio, determinata secondo regole e procedure in vigore presso l'organismo in cui egli presta servizio; le richieste di mezzi aggiuntivi devono essere sottoposte

all'approvazione del responsabile dell'amministrazione. Accordi di altra natura sono validi a patto che garantiscano al RPD le risorse di cui ha bisogno per l'espletamento della propria missione in modo indipendente;

- il RPD deve godere dei poteri di firma per tutta la corrispondenza relativa alla protezione dei dati.

Le autorità pubbliche degli Stati membri e la Autorità di protezione dei dati, qualora ne sia richiesto il parere, devono tenere in debito conto quanto finora enumerato al momento di decidere condizioni, accordi o contratti di applicazione nella nomina di un RPD, o di elaborare un parere in materia. Le DPA possono ritenere assolutamente appropriata anche l'elaborazione di guide dettagliate in materia, alla luce di quanto prima sottolineato.

Risorse e strutture

Il RGPD sancisce che:

> "Il titolare del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 [di cui si ritrova una lista alla sezione 2.3.4, *infra*] **fornendogli le risorse necessarie per assolvere tali compiti** e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica".
>
> (Articolo 38(2))

A tale proposito, il WP29 raccomanda in particolare:[289]

- sostegno attivo alle funzioni del RPD da parte delle alte dirigenze (come quelle a livello di Consiglio di Amministrazione);
- tempo sufficiente per l'espletamento delle funzioni di RPD. Questo elemento è di grande importanza laddove il RPD è nominato con un incarico a tempo parziale, o si occupa di protezione dei dati, ma anche di altre mansioni. In caso contrario, priorità in conflitto fra loro possono generare il non espletamento dei propri compiti da parte del RPD. E' di fondamentale importanza che il RPD abbia tempo sufficiente per il proprio lavoro ed è buona norma non solo stabilire una percentuale di tempo, qualora il RPD non lavori a tempo pieno in tale funzione, ma anche fissare il tempo necessario affinché egli porti a termine i propri compiti, stabilire un livello di priorità per le mansioni del RPD e per un piano di lavoro sia del singolo RPD che di tutta l'organizzazione in cui presta la propria opera;
- adeguato sostegno a livello di risorse finanziarie, infrastrutture (equipaggiamenti, servizi, spazi) e personale;
- comunicazione ufficiale della designazione del RPD a tutto il personale per garantire che la sua nomina e la sua funzione siano note in tutta l'organizzazione;
- accesso garantito ad altri servizi, come risorse umane, ufficio legale, IT, sicurezza, ecc., in modo che il RPD possa ricevere sostegno, aiuto e informazioni essenziali;
- Formazione continua [si veda *supra*, alla rubrica "*Formazione professionale e certificazioni*"];
- a seconda delle dimensioni e della struttura dell'organizzazione, può essere necessario creare una squadra di collaboratori a servizio del RPD. In tal caso, le strutture interne di questa squadra e i compiti e le responsabilità di ciascuno di coloro che ne faranno parte devono essere chiaramente definiti. Allo stesso modo, quando la funzione di RPD è esercitata da un fornitore esterno di servizi, un gruppo di collaboratori che lavorano per

289 Linee guida sui DPO del WP29 (nota 239, *supra*), sezioni 3.2, pp. 13 – 14.

> questa entità possono espletare le funzioni di un RPD collegialmente, sotto la responsabilità di un punto di contatto designato dal cliente.
>
> In generale, più complesse e/o sensibili le operazioni di trattamento, maggiori le risorse da fornire al RPD. La funzione di protezione dei dati deve essere efficace e godere di risorse proporzionate in relazione al trattamento dei dati da svolgere".

Come già rilevato, il Gruppo istituzionale dell'UE sui RPD ritiene che "un RPD che debba richiedere personale e risorse (risorse IT, budget per viaggi e formazione) al proprio superiore gerarchico possa ritrovarsi in difficoltà se il superiore in questione non è pienamente coinvolto nel raggiungimento della conformità della protezione dei dati." Il Gruppo, pertanto, raccomanda che il RPD abbia responsabilità di bilancio e che ogni richiesta di risorse aggiuntive venga approvata dall'organismo o dall'istituzione (piuttosto che da un diretto superiore gerarchico).[290]

Il CEDPO nota:

> "in organismi complessi, è necessario riflettere se il RPD debba essere coadiuvato o meno da altri collaboratori (che ne completino le competenze) in interno, su base permanente (la squadra dei collaboratori del RPD) o temporanea (un consiglio/gruppo esterno?).

Presso le autorità pubbliche la creazione di una squadra sarebbe una buona soluzione. Negli enti pubblici di piccole dimensioni, si tratterebbe semplicemente di collaboratori che si riuniscono con il RPD su base regolare per discutere le questioni principali ed elaborare politiche; in quelli di maggiori dimensioni, si possono creare (in modo più formale) delle funzioni di sostegno al RPD a tempo parziale; in altri può essere necessaria la nomina a tempo pieno di collaboratori che aiutino il RPD. Come chiariscono tutti i documenti di orientamento, tali decisioni devono essere prese: 1) alla luce della complessità e della sensibilità dei dati personali trattati e 2) alla luce delle dimensioni e delle risorse degli organismi in questione. Alla fine, comunque, è un requisito di legge fissato dal RGPD che le risorse attribuite al RPD (e alla sua squadra) siano adeguate ai compiti da svolgere.

I poteri del RPD

Oltre alle risorse e ad una posizione sufficientemente forte, alta e protetta in seno alla sua organizzazione, il RPD deve disporre anche di una serie di poteri per svolgere i propri compiti. L'Articolo 38(2) (citato nella precedente rubrica) chiarisce che, all'uopo, l'autorità che ha il potere di nomina del RPD deve garantirne l'"accesso" ai dati personali e alle attività di trattamento. Questo dispositivo è in linea con quello del Regolamento che tutela i RPD delle istituzioni dell'UE, Art. 24(6) del Regolamento (CE) 45/2001:[291]

> "il Regolamento chiede che i titolari assistano il RPD nell'esecuzione dei suoi compiti, forniscano le informazioni richieste e garantiscano che il RPD abbia sempre accesso ai

---

290 Si veda, *supra*, alla rubrica "*Posizione del RPD nella sua organizzazione*".

291 Rete dei RPD delle Istituzioni e degli Organismi dell'UE, Standard Professionali per i RPD delle Istituzioni e degli Organismi dell'UE che lavorano ai sensi del Regolamento (CE) 45/2001 (nota 241, *supra*), p. 12. Rileviamo che, a differenza dell'Art. 38(2) del RGPD, l'Art. 24(6) del Regolamento (CE) 45/2001 non fa espressa menzione all'accesso ai dati personali né alle attività di trattamento dei dati personali, due elementi che vanno letti alla luce della norma più generale che garantisce l'allocazione delle risorse necessarie. Il dispositivo risente probabilmente della norma (più specifica e più incisiva) sull'accesso a tali informazioni garantito (nelle istituzioni dell'UE) al GEPD.

> dati oggetto delle operazioni di trattamento e a tutte le strutture, le installazioni di trattamento dei dati e i supporti dati.
>
> Sebbene i RPD non abbiano poteri esecutivi nei confronti dei titolari, hanno comunque il potere di controllare la conformità tramite le raccolta di tutti i dati pertinenti che l'istituzione/ l'organismo che ha il potere di nomina e i suoi titolari hanno l'obbligo di fornire e rendere disponibili".

Anche altri commenti del Gruppo istituzionale dell'UE sui RPD e relativi all'obbligo di garanzia della conformità alle norme di protezione dei dati personali sono di grande importanza:[292]

> "per aiutare il RPD nelle sue attività periodiche di controllo devono essere sviluppati strumenti IT. Si possono anche prendere accordi a livello amministrativo, come garantire che il RPD riceva copia di ogni comunicazione in materia di protezione dei dati e chiedere che egli venga consultato su ogni documento che ne tratti. Un monitoraggio attento e regolare della conformità e la presentazione dei risultati possono esercitare una forte pressione sui titolari per garantire la conformità delle loro operazioni di trattamento. Il monitoraggio periodico e il reporting dei risultati sono l'arma più forte a disposizione del RPD per garantire la conformità e, a questo scopo, una relazione annua destinata alle alte dirigenze costituisce un'ottima prassi".

Un problema a parte è quello del titolare o del responsabile che rifiutino di seguire il parere del RPD. Il WP29 afferma:[293]

> "se il titolare o il responsabile prendono decisioni incampatibili con il RGPD e con il parere del RPD, il RPD deve avere facoltà di manifestare il proprio parere discorde al vertice gerarchico e ai responsabili delle decisioni. In tal senso, l'Articolo 38(3) stabilisce che il RPD 'riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento'. Questo reporting diretto garantisce che il vertice gerarchico (ad es., il Consiglio di Amministrazione) conosca il parere del RPD e le raccomandazioni che costituiscono parte integrante della missione del RPD di informare e consigliare il titolare o il responsabile. Un altro esempio di reporting diretto è la relazione annua delle attività del RPD destinata ai vertici gerarchici di più alto livello.

Sebbene non ci siano norme specifiche nel RGPD sull'obbligo, per i RPD, di riferire alle autorità i casi di non conformità alla legge, il RGPD sancisce comunque che questo è uno dei compiti del RPD:

> "fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, […], ed **effettuare, se del caso**, consultazioni relativamente a qualunque altra questione" (Art. 39(1)(e), grassetto aggiunto).

Nei casi in cui il RPD abbia l'impressione che il suo datore di lavoro agisca in violazione della legge, ha certamente facoltà – in effetti, diremmo, il dovere – di sollevare la questione con la DPA nazionale e di risolverla, una situazione che ben illustra la delicatezza di questa funzione.

Il WP29 sottolinea, e a giusto titolo, che:[294]

---

292 *Idem*.

293 Linee guida sui RPD del WP29 (nota 239, *supra*), p. 15. Lo stesso approccio è quello della Rete dei RPD delle Istituzioni e degli Organismi dell'UE, Standard Professionali per i RPD delle Istituzioni e degli Organismi dell'UE che lavorano ai sensi del Regolamento (CE) 45/2001 (nota 241, *supra*), p. 12 (si veda il paragrafo successivo a quello citato nel testo, *supra*).

294 Linee guida sui DPO del WP 29, p. 15, con un riferimento al principio di "responsabilizzazione" di cui all'Art. 5(2) del RGPD.

> "l'autonomia dei RPD, comunque, non significa che godano di poteri decisionali che oltrepassino gli ambiti stabiliti dall'Articolo 39.
>
> Il titolare o il responsabile rimangono i responsabili della conformità alla legislazione sulla protezione dei dati e devono essere in grado di dimostrare tale conformità".

Aspetti formali

Tutte le norme che riguardano la figura e le attività del DPO devono trovare rispecchiamento in maniera inequivocabile nei documenti della sua nomina. Come afferma l'Autorità italiana sulla protezione dei dati, il *Garante della Privacy*, nelle sue FAQ sui DPO:[295]

> "il RGPD prevede all'art. 37, par. 1, che il titolare e il responsabile del trattamento designino il RPD; da ciò deriva, quindi, che l'atto di designazione è parte costitutiva dell'adempimento.
>
> Nel caso in cui la scelta del RPD ricada su una professionalità interna all'ente, occorre formalizzare un apposito atto di designazione a "Responsabile per la protezione dei dati". In caso, invece, di ricorso a soggetti esterni all'ente, la designazione costituirà parte integrante dell'apposito contratto di servizi redatto in base a quanto previsto dall'art. 37 del RGPD (…).
>
> Indipendentemente dalla natura e dalla forma dell'atto utilizzato, è necessario che nello stesso sia individuato in maniera inequivocabile il soggetto che opererà come RPD, riportandone espressamente le generalità, i compiti (eventualmente anche ulteriori a quelli previsti dall'art. 39 del RGPD) e le funzioni che questi sarà chiamato a svolgere in ausilio al titolare/responsabile del trattamento, in conformità a quanto previsto dal quadro normativo di riferimento.
>
> L'eventuale assegnazione di compiti aggiuntivi, rispetto a quelli originariamente previsti nell'atto di designazione, dovrà comportare la modifica e/o l'integrazione dello stesso o delle clausole contrattuali.
>
> Nell'atto di designazione o nel contratto di servizi devono risultare succintamente indicate anche le motivazioni che hanno indotto l'ente a individuare, nella persona fisica selezionata, il proprio RPD, al fine di consentire la verifica del rispetto dei requisiti previsti dall'art. 37, par. 5 del RGPD, anche mediante rinvio agli esiti delle procedure di selezione interna o esterna effettuata. La specificazione dei criteri utilizzati nella valutazione compiuta dall'ente nella scelta di tale figura, oltre a essere indice di trasparenza e di buon amministrazione, costituisce anche elemento di valutazione del rispetto del principio di «responsabilizzazione».
>
> Una volta individuato, il titolare o il responsabile del trattamento è tenuto a indicare, nell'informativa fornita agli interessati, i dati di contatto del RPD pubblicando gli stessi anche sui siti web e a comunicarli al Garante (art. 37, par. 7). Per quanto attiene al sito web, può risultare opportuno inserire i riferimenti del RPD nella sezione "amministrazione trasparente", oltre che nella sezione "privacy" eventualmente già presente".

> Come chiarito nelle Linee guida [del Gruppo Art.29], in base all'art. 37, par. 7, non è necessario (anche se potrebbe costituire una buona prassi in ambito pubblico) pubblicare anche il nominativo del RPD, mentre occorre che sia comunicato al Garante per agevolare i contatti con l'Autorità. Resta invece fermo l'obbligo di comunicare il nominativo agli interessati in caso di violazione dei dati personali (art. 33, par. 3, lett. b).

2.5.4 Funzioni e compiti del RPD (panoramica)

[295] *Garante*, FAQ sui DPO (nota 246, *supra*), sezione 1. Il *Garante* allega alle FAQ una **scheda di atto di designazione del RPD.** A scopo facilitativo, viene allegata anche una '**Scheda per la comunicazione dei dati del RPD al Garante**'.

Riagganciandosi alla Rete istituzionale dell'UE sui RPD, il GEPD ha individuato le seguenti **sette funzioni che caratterizzano il RPD**:[296]

- informazione e sensibilizzazione;
- consulenza;
- procedure organizzative;
- procedure cooperative;
- garanzia del rispetto della conformità;
- trattamento delle controversie e dei reclami;
- funzioni di controllo e applicazione normativa.

I RPD designati ai sensi del RGPD svolgono compiti con funzioni assolutamente simili e correlate a **compiti** più specifici, indicati a grandi linee all'Articolo 39 del RGPD:

Articolo 39

Compiti del Responsabile della protezione dei dati

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;

(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;

(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;

(d) cooperare con l'autorità di controllo;

(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.

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.

In concreto, i RPD saranno naturalmente coinvolti in alcune attività che formalmente spettano al rispettivo titolare o responsabile, poiché molti titolari o responsabili (a meno che abbiano approfondite competenze in materia al di là di quelle possedute dal loro RPD, per

[296] GEPD, Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001 (nota 241, *supra*), pp. 6 – 7.

esempio attraverso i servizi giuridici o di compliance di cui dispongono) cercheranno il supporto del RPD nello svolgimento delle attività in oggetto. In realtà, a ben vedere, i titolari o responsabili posti dinanzi alle nuove e importanti incombenze che derivano dal RGPD (soprattutto dai nuovi obblighi di responsabilizzazione) tenderanno a chiedere al RPD di svolgere buona parte delle attività necessarie – anche se, come previsto espressamente dal RGPD e chiarito in più frangenti, la responsabilità di eventuali mancanze al riguardo resta sempre legalmente in capo al titolare, e non al RPD. Nello specifico, come chiarisce l'Articolo 5(2) del RGPD:

> "Il *titolare del trattamento* è competente per il rispetto delle [varie disposizioni del RGPD] e in grado di comprovarlo".

In altri termini, tale responsabilità non grava sulle spalle del RPD – e questo emerge chiaramente anche dall'Articolo 39, già citato, che sottolinea i compiti di consulenza e di sostegno del RPD.

Il RPD, comunque, svolge un ruolo cruciale da questo punto di vista in quanto, tramite i suoi pareri, deve orientare i vertici gerarchici e il personale di livello inferiore all'ottemperanza dei requisiti di legge. Viceversa, sia la dirigenza ai vertici che a livello più basso ha l'obbligo di consultare il RPD qualora emergano problemi di conformità al RGPD.

Il GEPD ha elaborato, all'uopo, una matrice molto utile, nota come RACI ("**R**esponsible, **A**ccountable, **C**onsulted, **I**nformed") che può essere utilizzata, in particolare, nella tenuta dei registri o delle registrazioni delle operazioni di trattamento dei dati personali:[297]

	Responsible	Accountable	Consulted	Informed
Top Management		**X**		
Referente	**X**			
RPD			**X**	
Dipartimento IT			**X**	
Responsabili, se del caso			**X**	

Il GEPD ha poi aggiunto il seguente chiarimento terminologico:[298]

> '**Responsible'** è colui che ha l'obbligo di azione e di decisione per il raggiungimento dei risultati richiesti; '**Accountable'** è colui che risponde delle azioni, delle decisioni e della prestazione; '**Consulted'** è colui al quale è richiesto di contribuire e fornire commenti;

---

297 GEPD, Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments, febbraio 2018, p. 4: https://edps.europa.eu/sites/edp/files/publication/18-02-06_accountability_on_the_ground_part_1_en_0.pdf Nella colonna di sinistra si può aggiungere anche "Soggetti interessati" e "Autorità di protezione dei dati", con una "X" per coloro che figurano nell'ultima colonna ("Informati"), ma i compiti reali sono molto più complessi di quelli indicati con questo sistema: gli interessati devono, infatti, ricevere informazioni su determinate questioni e in determinati casi (sia dal titolare, *motu proprio*, o su richiesta), ma non sempre essere informati di tutto, e la DPA, in alcuni casi, non deve essere informata, ma consultata. La matrice ha comunque lo scopo di chiarire eventuali criticità all'interno dell'organizzazione dei titolare, e non tanto in organismi esterni.

298 *Idem*, nota 7 (grassetto aggiunto).

'**Informed'** è colui che viene mantenuto informato delle decisioni prese e del trattamento.

Il GEPD utilizza il termine "**referente dell'attività**" per la persona che, nella pratica quotidiana, è responsabile di tutte le attività di trattamento: il "proprietario" del trattamento. Come avremo modo di chiarire alla rubrica "*Compito preliminare*", una delle prime mansioni del RPD consiste proprio nel fare una mappatura della ripartizione interna di queste responsabilità.

In linea con quanto rilevato nello spaccato generale dei compiti del RPD, vedi *infra*, tali compiti spesso figurano come mansioni di "aiuto al titolare" per garantire tutta una serie di elementi, oppure come "consulenza al titolare" (o al "referente dell'attività"/membro del personale responsabile) per raggiungere determinati fini, piuttosto che come "garanzia" del conseguimento di un risultato o "imposizione" di soluzioni. In pratica, soprattutto nelle organizzazioni più piccole, può accadere che il DPO porti avanti la maggior parte di queste mansioni da solo, anche se, formalmente, esse restano di responsabilità del titolare (e, all'interno dell'oraganizzazione, del "referente dell'attività"/membro del personale responsabile).

Da quanto precede, e tenendo presente quanto osservato rispetto alla limitata responsabilità del RPD, si evincono **quindici compiti a carico del RPD (o che di fatto vedono il coinvolgimento del RPD)** (più un *Compito preliminare*), che possono essere raggruppati nelle sette funzioni principali identificate dal GEPD, come indicato nell'introduzione alla Parte III del Manuale.

Questi compiti e queste funzioni sono tutti, a loro volta, strettamente legati al principio di "**responsabilizzazione**" e a quello, associato, di "**dimostrazione degli obblighi di conformità**" imposti al titolare e discussi alla sezione 2.2 di questo Manuale (vedi *supra*).

Nella prossima parte di questo Manuale (la Parte III) forniremo orientamenti sulle modalità di assolvimento di tali compiti da parte di titolari e RPD. Prima di tutto, però, è importante ricordare che, benché il RPD eserciti grande influenza sullo svolgimento di tali compiti, egli non ha alcuna responsabilità formale o personale per la conformità al RGPD.

Ovviamente, il RPD dovrà definire una strategia per far fronte a tutti i compiti in questione, sulla base di un programma semestrale o annuale, con una certa flessibilità per tener conto di eventuali imprevisti (un improvviso problema di protezione dati, oppure una violazione dei dati personali a carico dell'ente, oppure un'ispezione decisa dall'autorità di controllo).

- o – O – o –

PARTE TERZA

Guida pratica sui compiti del RPD
ovvero ciò che in pratica il RPD dovrà fare
("I compiti del RPD")

Questa parte del manuale mira a fornire una guida pratica sui **compiti del RPD, ovvero sulle attività in cui sarà in pratica coinvolto il RPD,** così come già descritto nella sezione precedente 2.5.4, e nelle pagine successive. Per brevità, di volta in volta, ci riferiremo ad essi come a "i compiti del RPD". Come osservato nella precedente sezione, i quattordici compiti derivano dalla lista di quelli previsti in termini generali dall'art. 39 del RGPD, raggruppati secondo il criterio delle **sette funzioni del RPD,** così come identificate dal GEPD. Nelle varie sezioni che trattano i compiti del RPD, si forniscono esempi illustrativi legati alla pratica attuale.

I compiti del RPD:

Compito preliminare:

Delineare il contesto in cui opera il titolare

Funzioni organizzative:

Compito 1: Creazione di un registro delle attività di trattamento

Compito 2: Verifica delle attività di trattamento di dati personali

Compito 3: Valutazione dei rischi posti dalle attività di trattamento di dati personali

Compito 4: Gestione dei trattamenti che possono comportare un "rischio elevato": come si conduce una valutazione d'impatto sulla protezione dei dati (Data Protection Impact Assessment - DPIA)

Controllo della conformità:

Compito 5: Ripetizione dei compiti 1-3 (e 4) su base continuativa

Compito 6: Gestione delle violazioni dei dati personali (data breach)

Compito 7: Compiti di indagine (compresa la gestione dei reclami interni)

Funzioni consultive:

Compito 8: Funzioni di consulenza – aspetti generali

Compito 9: Sostegno e promozione dei principi di "Data Protection by Design & Default"

Compito 10: Consulenza e monitoraggio della conformità delle politiche di protezione dei dati, dei contratti tra contitolari, tra titolari, e tra titolare e responsabile, norme vincolanti d'impresa, e clausole per il trasferimento dati

Compito 11: Coinvolgimento nei codici di condotta e nelle certificazioni

Cooperazione con e consultazione dell'autorità di protezione dati

Compito 12: Cooperazione con l'autorità di protezione dati

Gestione delle richieste dell'interessato:

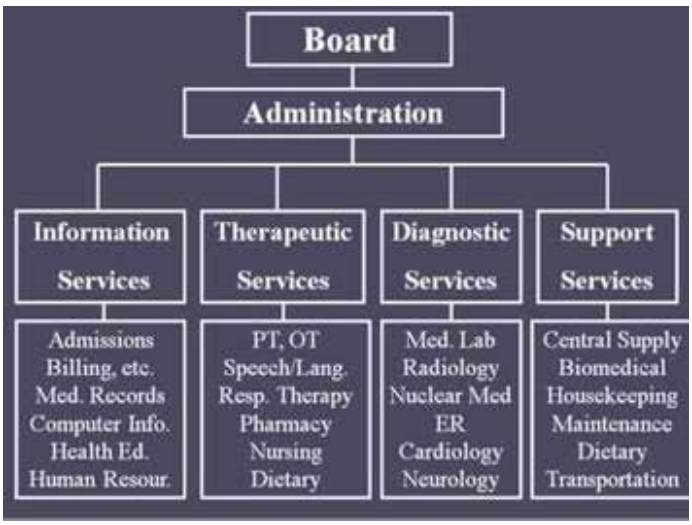
Compiti preliminari:

Compito preliminare del RPD: esame del contesto in cui opera il titolare e mappatura generale delle attività di trattamento dell'organizzazione

Un RPD può svolgere i propri compiti rispetto al proprio datore di lavoro se è pienamente consapevole: i) della distribuzione **interna** e dell'allocazione dei compiti e delle responsabilità relative a ciascun trattamento di dati personali; ii) dei legami **esterni** e degli accordi che tale organizzazione ha con altre organizzazioni; iii) del loro quadro **giuridico**. Prima di intraprendere gli altri compiti principali che gli spettano – fatta eccezione per la predisposizione dell'inventario iniziale (registro) delle attività di trattamento, enumerato per primo nella prossima sezione (Compito 1) e che può essere effettuato in parallelo - il RPD è tenuto pertanto a definire legami interni ed esterni e segmenti di responsabilità riguardo a ciascun trattamento, collocandoli nel più ampio contesto del ruolo e delle finalità dell'organizzazione, e familiarizzando a fondo con le regole rilevanti.

Per chiarire le strutture **interne** e i ruoli, il RPD deve prima di tutto ottenere e studiare l'**organigramma** della propria organizzazione, che l'amministrazione dovrebbe essere in grado di fornirgli.

ESEMPIO: Organigramma di un ospedale



Fonte: *Principles of Health Science*, https://www.youtube.com/watch?v=FpQEwbAV3Qw

Di norma gli organigrammi identificheranno solamente le unità rilevanti e i dipartimenti in termini generali: "risorse umane", "finanza e contabilità", "affari legali", "gestione clientela", ecc. (molti enti pubblici adotteranno peraltro la terminologia delle entità private, ad esempio riferendosi ai beneficiari di sussidi o assistenza come ai "clienti" dell'ufficio pubblico). Si tratta di un utile punto di partenza, ma non molto più di questo. Attraverso discussioni approfondite con l'alta dirigenza, compresi i responsabili legali e delle risorse tecnologiche e, ove appropriato, gli uffici regionali o nazionali, il RPD dovrebbe chiarire con maggior dettaglio quali sono le responsabilità delle diverse unità e dipartimenti, in particolare per quali finalità ogni unità e dipartimento necessita di, ed effettivamente tratta, dati personali; con quale architettura di tecnologie interne ed esterne ciò viene fatto; e se ciò comporta servizi o mezzi tecnologici esterni (compreso il cloud computing). È qui che l'esame preliminare si

sovrappone alla predisposizione del registro delle attività di trattamento previsto nel compito 1 – anche se, ad uno stadio preliminare, le attività di trattamento rilevanti devono essere identificate solamente in termini generali, con riferimento alla finalità di ciascuna operazione e le tecnologie utilizzate.

Inoltre, il RPD in questa fase preliminare dovrebbe aver maturato un'idea iniziale di quali specifici **compiti** e **responsabilità** spettano a ciascuna unità o dipartimento in relazione a ciascun trattamento, ovvero dovrebbe identificare chi è il "referente" di ciascuna attività di trattamento (per usare la terminologia del GEPD).

ESEMPI:[299]

L'autorità di protezione dei dati spagnola, la AEPD, enumera i seguenti **esempi di registri ufficiali (richiesti per legge) di dati personali tenuti dalle autorità locali**:

- Registro anagrafico
- Registro dei contribuenti locali
- Registro dei destinatari di sussidi (ad es. sussidi per l'alloggio o per disabilità)
- Registro di beneficiari di servizi sociali (ad es. prestazioni per minori)
- Registri delle sanzioni amministrative (ad es. multe per parcheggio non autorizzato)
- Registro delle licenze e permessi rilasciati (ad es. per la gestione di un locale)
- Registro delle unità e dei funzionari di polizia locale
- Registro di persone iscritte agli uffici di collocamento delle autorità locali;
- Registro dei minori che usufruiscono dei servizi scolastici locali
- Registro di stato civile
- Registro delle persone sepolte nei cimiteri locali
- Registro degli utenti di biblioteche gestite da autorità locali
- Registro di persone iscritte a servizi di notificazione di eventi culturali

Così come, ovviamente:

- Contabilità
- Risorse umane
- eccetera

L'autorità di protezione dati fornisce i seguenti esempi di leggi o regolamenti che sono alla base di trattamenti di dati personali in relazione ad alcuni dei registri mantenuti dalle autorità locali spagnole citati sopra: [300]

Registro:	Normativa primaria/secondaria di riferimento:
• Registro anagrafico	Legge sul registro anagrafico
• Registro dei contribuenti	Legge sulle *haciendas*
• Registro del personale	Regolamenti relativi a questa attività

[299] Gli esempi si basano sulla guida settoriale predisposta dall'autorità di protezione dati spagnola, AEPD: *Protección de Datos y Administración Local*, 2017, p. 8 (nostra traduzione e riformulazione), disponibile su: https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf

[300] Cfr. Guida settoriale spagnola su protezione dati e amministrazioni locali, nota precedente, p. 11.

In alcune circostanze, potrebbero esserci altre basi giuridiche per il trattamento, ad es.:

Registro:	Altre basi giuridiche:
• Registro di iscritti a servizi di notificazione di eventi culturali	Consenso e regolamentazione locale
• Registro degli utenti di biblioteche gestite da autorità locali	Contratto e regolamentazione locale

È inoltre importante che in questa fase il RPD (con l'aiuto del personale informatico e della sicurezza) acquisisca familiarità con i **sistemi ICT, l'architettura e le politiche della propria organizzazione**: i computer (o, ove ancora utilizzati, i sistemi di archiviazione manuale) utilizzati e se essi includono dispositivi portatili e/o mobili (e/o "dispositivi propri" del personale – per i quali deve essere predisposta una policy "Bring Your Own Device [BYOD]"); se i computer o i dispositivi personali sono utilizzati online o solamente offline, in loco o anche da remoto; quale software per la sicurezza e crittografia è utilizzato e se è pienamente aggiornato; quali servizi esterni vi sono (incluso l'impiego di server cloud, specie se stabiliti fuori dall'UE/SEE, ad es. negli Stati Uniti - nel qual caso i rilevanti accordi e contratti per i trasferimenti di dati devono essere vagliati); se alcuno dei trattamenti è effettuato da responsabili (nel qual caso i contratti con essi dovranno essere vagliati);[301] quali sono le misure di sicurezza fisiche (porte, stanze, password di rete e PC, ecc.), se sono in essere policy e attività di formazione sulla sicurezza, ecc. In questa fase preliminare non è necessario che tutte le questioni menzionate siano risolte, ma devono quantomeno essere **considerate, mappate e registrate**.

Nella fase successiva, il RPD dovrebbe cercare di chiarire tutti i legami **esterni** che la propria organizzazione ha con altre. Tali organizzazioni sono di norma di **due tipologie:** a) organizzazioni (sorelle/madri/figlie) con le quali quella del RPD ha legami formali, nell'ambito di ciò che di norma sarà (nel settore pubblico) **l'organizzazione complessiva dell'attività amministrativa**. Un'autorità locale potrebbe formalmente ricadere sotto l'immediata giurisdizione di un ente regionale, che a sua volta è sotto il controllo o la supervisione di un ente provinciale o federale, che al più alto livello si inserisce all'interno di una più ampia amministrazione pubblica nazionale, al di sotto di un ministero nazionale. Ci saranno

---

301 L'autorità per la protezione dei dati personali spagnola, AEPD, in un contributo per questo manuale, fornisce i seguenti **esempi** di attività di trattamento che sono spesso subappaltate dalle autorità locali (ovvero, nella prospettiva della protezione dei dati, ove il trattamento sia effettuato da un responsabile):
• La preparazione dei libri paga del personale
• La distruzione di documentazione o dei relativi supporti
• Il controllo delle video-camere di sorveglianza
• La gestione della riscossione delle tasse
• La manutenzione dell'attrezzatura informatica
• Il trattamento dei dati relativi al Registro anagrafico municipale
• Il trattamento dei dati relativi alle tasse municipali
• Il trattamento dei dati relativi al personale: per quanto applicabile alla disciplina delle amministrazioni pubbliche
• La sottoscrizione attraverso un servizio offerto da un consiglio comunale sul proprio sito per ricevere comunicazioni relative ad attività culturali
• Iscrizione in un un'agenzia per l'impiego
(La AEDP considera anche il cloud computing, come già notato nel testo).

naturalmente grandi differenze tra stato e stato, o anche all'interno di uno stesso stato, anche per ciò che concerne la relativa autonomia che i diversi enti hanno, e in relazione all'avvio e alla gestione delle loro attività di trattamento; è esattamente questa la ragione per cui il RPD dovrebbe familiarizzare a fondo con gli assetti particolari della propria organizzazione specifica.

Il quadro di riferimento per tutti gli enti pubblici rilevanti che appartengono ad una determinata gerarchia sarà ampiamente definito nel **diritto formale**, con i suoi diversi livelli: Costituzione,

legge positiva, atti normativi (legislazione secondaria vincolante), ordinanze e circolari ministeriali, così come eventuali **accordi amministrativi** non vincolanti o non basati su atti di legge, altri accordi,[302] linee-guida e dichiarazioni politiche, ecc. Il trattamento dei dati personali effettuato dall'organizzazione del RPD potrebbe essere altresì coperto da un codice di condotta, di cui esistono diversi tipologie. Di nuovo, il RPD dovrebbe acquisire una comprensione, la più completa e dettagliata possibile, di quegli accordi, codici e regole, e dei processi attraverso i quali sono adottati, applicati, rivisti ed emendati; anche qui, se necessario, avvalendosi del supporto degli esperti legali della sua organizzazione (e/o attraverso la frequenza di corsi sulle tematiche rilevanti).

Data la presenza di altri RPD nelle organizzazioni omologhe, sarà fondamentale per il "nostro" RPD divenire parte integrante di una **rete di RPD.** Ove non vi sia tale rete, il RPD dovrebbe lavorare per la sua creazione. Tutti i RPD dovrebbero naturalmente stabilire **un buon rapporto con l'autorità nazionale di protezione dati,** in particolare con i dirigenti all'interno dell'autorità, dotati di specifiche responsabilità con riferimento alle autorità pubbliche e al tipo di autorità pubblica cui appartiene il RPD.

Gli accordi fatti dall'autorità di protezione dati francese, la CNIL, per una rete nazionale di RPD, con una "extranet" dedicata, è un buon esempio di autorità che supporta questo tipo di networking e interazione.[303]

Ci sono poi i legami con le **organizzazioni esterne che sono al di fuori della struttura gerarchica cui appartiene RPD.** Tali organizzazioni possono ricomprendere altre **autorità pubbliche che si collocano in una differente gerarchia;** ad esempio, possono esserci rapporti tra istituzioni scolastiche e quelle dedicate al welfare, o quelle di polizia, oppure tra autorità scolastiche di un determinato paese con omologhe organizzazioni di un altro paese. Anche in questo caso, i rapporti con tali enti sono (o dovrebbero essere) disciplinati da norme di legge o da altre intese o accordi formali vincolanti (ad esempio ai fini di scambio di dati tra amministrazioni o della disciplina dei rapporti tra istituti scolastici e sistema del welfare). Il RPD dovrebbe, di nuovo, acquisire piena conoscenza di tali accordi ogni volta che essi implichino il trattamento di dati personali – e dovrebbe di fatto riesaminarli, per verificare se adeguatamente riflettono, confermano e implementano i requisiti del RGPD e delle altre normative e regole nazionali sulla protezione dei dati, nonché della normativa sui diritti

---

302 Tali accordi potrebbero includere gli accordi tra enti pubblici in base ai quali un ente pubblico tratta dati personali per conto di un altro, ovvero agisce in qualità di responsabile del trattamento per quest'ultimo. Si veda la discussione nel testo sui contratti fra titolari, e fra titolare e responsabile e ai fini del trasferimento dei dati

303 Si veda la sezione 2.5.3, "*Formal training and certification"* e la nota 271.

umani.[304] Il RPD probabilmente non avrà il potere di contestare una normativa lacunosa in quanto tale, ma potrebbe – e dovrebbe – informare il proprio datore di lavoro, e probabilmente l'autorità di protezione dati competente, del proprio punto di vista sulla lacunosità della legge.

Talvolta, i rapporti e la cooperazione tra entità formalmente distinte sono fondate su **accordi informali e non pubblici**. Tuttavia, ciò può essere problematico dal punto di vista della protezione dei dati.

Come osservato dal Gruppo art. 29 nel suo parere sulla nozione di titolare e responsabile:[305]

> [Esiste] una crescente tendenza alla differenziazione organizzativa nella maggior parte dei settori interessati. Nel settore privato, la ripartizione dei rischi, finanziari o d'altro tipo, ha portato ad una continua diversificazione delle imprese, ancora più accentuata da fusioni e acquisizioni. Nel settore pubblico una differenziazione analoga sta avendo luogo nell'ambito del decentramento o della separazione dei servizi politici e delle agenzie esecutive. In entrambi i settori viene accordata sempre più importanza allo sviluppo di catene di prestazione di servizi o alla prestazione di servizi inter-organismi, e al ricorso al subappalto o all'esternalizzazione di servizi per beneficiare di specializzazione e di eventuali economie di scala. Il risultato è un proliferare di vari servizi, e i prestatari che li offrono non sempre si considerano responsabili o tenuti a rendere conto del proprio operato. In funzione delle scelte organizzative delle imprese (e dei loro appaltatori o subappaltatori), le banche dati rilevanti possono trovarsi in uno o più paesi nell'Unione europea o al di fuori.

Un simile quadro crea difficoltà nella ripartizione delle responsabilità e nell'attribuzione della titolarità. Il Gruppo art. 29 ha sostenuto che le entità coinvolte dovrebbero fornire "sufficiente chiarezza" nella suddivisione delle responsabilità e nell'effettiva attribuzione di (varie forme e livelli di) titolarità – che in pratica significa che le entità coinvolte dovrebbero **discutere** di tali questioni, **accordarsi** su tali ripartizioni e attribuzioni, e **registrare** il tutto in un **accordo formale** che può (e su richiesta ovviamente dovrebbe) essere fornito alla/e autorità di protezione dati competente/i e (forse in una forma semplificata) agli interessati e al pubblico.

Come parte del compito preliminare di definizione dell'ambito delle attività del titolare, il RPD dovrebbe, di nuovo, **verificare** se esistono tali tipi di accordi formali, e in caso positivo, se essi a) riflettono veramente la ripartizione pratica e le attribuzioni di responsabilità e b) rispettano pienamente i requisiti del RGPD. Se non vi sono accordi formali, il RPD dovrebbe **consigliarne** l'urgente predisposizione (con il suo coinvolgimento nella discussione, nell'accordo e nella registrazione). Se vi sono solamente accordi informali, il RPD dovrebbe **consigliarne** la sostituzione con accordi formali.

Inoltre, quando i rapporti con altre entità includono accordi tra titolari e tra titolare e responsabile, dovrebbero essere rispettivamente regolati da specifici contratti (conformi al

---

304 Si veda la sentenza della Corte europea dei diritti dell'uomo Copland v. UK del 3 aprile 2007, nella quale la Corte ha sostenuto che una disposizione normativa formulata in maniera non sufficientemente precisa in una legge che concede a un'autorità pubblica un'ampia competenza in un determinato settore non costituisce "legge" ai sensi della Convenzione europea dei diritti dell'uomo (http://hudoc.echr.coe.int/eng?i=001-79996 (si veda in particolare il paragrafo 47.)

305 Gruppo art. 29, Parere 1/2010 (WP169, adottato il 16 febbraio 2010), pag. 6, e disponibile al link: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

RGPD); e ove le relazioni e gli accordi con altre entità comportino trasferimenti di dati personali verso paesi extra UE/AEE (cd "paesi terzi"), i trasferimenti dovrebbero basarsi su apposite clausole (conformi al RGPD) (clausole standard approvate dalla/e autorità competente/i o dal CEPD, o clausole ad hoc conformi al RGPD.

Quando sussistono tali contratti o clausole, il RPD dovrebbe **riesaminarli** per verificarne la conformità al RGPD, e ove invece non vi siano, il DPO dovrebbe **consigliarne** l'urgente stipulazione ove necessario.

Questi compiti del RPD relativi ad accordi formali, contratti e clausole tra titolari e tra titolare e responsabile (anche con riferimento ad altri aspetti) sono discussi più approfonditamente, nel punto 3.10. Qui, sarà sufficiente notare che il RPD dovrebbe **identificare** tali questioni nel compito preliminare di definizione dell'ambito delle attività del titolare, per poi affrontarle da quel momento in poi.

Infine, l'organizzazione del RPD avrà **rapporti con fornitori esterni (del settore pubblico e privato) di beni o servizi**, dai trattamenti dati in outsourcing, alla contabilità e gestione del sito web, alla fornitura di pasti mensa, manutenzione e riparazioni, supporto medico e benessere del personale, ecc. Le attività svolte in tali ambiti si fonderanno su **contratti** (ordinari contratti di diritto privato o contratti di partenariato pubblico-privato). Tali contratti rappresenteranno la base anche per (e dovrebbero specificamente) coprire qualunque trattamento di dati personali effettuato dalle parti: dalla raccolta dei rilevanti dati personali alla condivisione e all'utilizzo di quei dati, fino alla loro distruzione finale o cancellazione. Se l'altra entità è titolare, tali contratti (o almeno gli elementi di quei contratti, rilevanti per la protezione dei dati) costituiranno nel linguaggio della protezione dei dati, contratti di trattamento dati **fra titolari**. Se l'altra entità agisce semplicemente come responsabile per l'organizzazione del RPD, il contratto sarà un contratto **titolare-responsabile**. E se in base al contratto, dati personali sono trasferiti in un luogo al di fuori dell'UE/AEE (tipicamente, verso un server "cloud" gestito dal contraente), tali contratti costituiscono **contratti per il trasferimento dei dati personali**.

Nell'esercizio preliminare di definizione dell'ambito delle attività del titolare, il RPD dovrebbe di nuovo **identificare** se esistono tali contratti e, subito dopo tale esercizio, **esaminarli**, così che ove risultino assenti o non pienamente conformi al RGPD, **possa consigliarne** la predisposizione o la revisione.

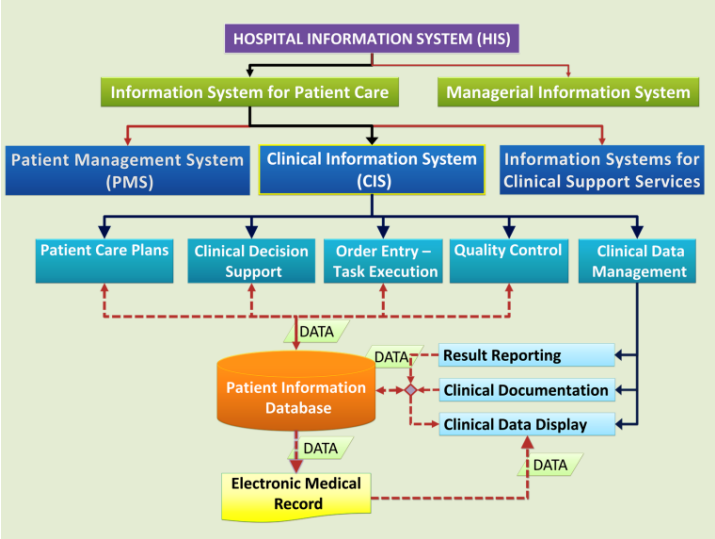
Mappatura generale delle attività di trattamento dell'organizzazione

Dopo aver effettuato la definizione dell'ambito di attività della propria organizzazione (come indicato sopra), il RPD sarà in grado di rilevare le attività di trattamento di dati personali dell'organizzazione in termini generali, come passo cruciale verso la creazione di un registro dettagliato di tutte quelle attività e di tutte le operazioni di trattamento di dati personali, effettuata nel Compito 1 (vedi *infra*). Ciò dovrebbe portare ad un diagramma come quella riportato qui sotto, che spiega "le componenti funzionali di un sistema informativo clinico".[306]

ESEMPIO:

[306] Luigi Carrozzi, presentazione nel corso della prima sessione di formazione del "T4DATA", giugno 2018: "*Linee-guida pratiche per i RPD – Il registro delle operazioni di trattamento*".

Mappatura delle attività di trattamento dati effettuate da un'organizzazione (qui un ospedale)



Fonte: Abdollah Salleh, https://drdollah.com/hospital-information-system-his/

Si noti che la tabella sopra indicata si riferisce maggiormente alle operazioni di trattamento dati piuttosto che all'organigramma di un ospedale, riportato in precedenza.

Compiti organizzativi:

Compito 1: La creazione di un registro delle attività di trattamento di dati personali

Fatta salva la limitata esenzione discussa nella relativa sezione, prevista dall'art. 30 del RGPD, ogni titolare deve tenere "un **registro** delle attività di trattamento svolte sotto la propria responsabilità", contenente vari dettagli di ciascuna operazione, quali il nome del titolare (e, si potrebbe aggiungere, del "referente"), le finalità del trattamento, le categorie di interessati, di dati personali, di destinatari, ecc. L'obbligo di tenere un registro delle operazioni di trattamento è strettamente legato al principio di *accountability* discusso nella sezione 2.2, facilitando esso l'efficace supervisione da parte della competente autorità di protezione dei dati ("autorità di controllo"), come sottolineato dal considerando 82 del RGPD:[307]

> ***Per dimostrare che si conforma*** *al presente regolamento, il titolare del trattamento o il responsabile del trattamento* ***dovrebbe tenere un registro delle attività di trattamento*** *effettuate sotto la sua responsabilità.*
>
> ***Sarebbe necessario obbligare*** *tutti i titolari del trattamento e i responsabili del trattamento* ***a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione*** *affinché possano servire per monitorare detti trattamenti.*

In altre parole, come detto dall'autorità di protezione dei dati italiana:[308]

> **[Il registro è una] misura per dimostrare la conformità al RGPD**

Il riferimento alle "attività di trattamento svolte sotto la (…) responsabilità [del titolare]" suggerisce che lo stesso registro deve coprire **tutte** le operazioni di trattamento, e ciò è infatti espressamente previsto dalla versione tedesca del RGPD.[309] Anche questo è significativo, posto che, come anche il Garante sottolinea:[310]

> Il quadro complessivo delle informazioni che si qualificano come "dati personali" e le relative operazioni di trattamento fornite dal registro costituiscono il **primo passo verso la accountability** in quanto consentono di valutare i rischi sui diritti e la libertà delle persone e di attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Nonostante, come la maggior parte degli altri requisiti del RGPD, questo sia formalmente un dovere del titolare piuttosto che del RPD, in pratica sarà proprio il RPD ad essere chiamato a svolgere tale lavoro (in stretta cooperazione con il competente staff del titolare), o ad essere

---

307 Luigi Carrozzi, presentazione tenuta in occasione della prima sessione di formazione "T4Data", giugno 2018, relativamente a "Indicazioni pratiche per i RPD – Il registro delle attività di trattamento".

308 *Idem*.

309 "*Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen.*".

310 Luigi Carrozzi, cit. (cfr. nota 307, *supra*).

quantomeno fortemente coinvolto nello svolgimento di tale compito e della sua supervisione. Come sostiene il Gruppo art. 29 (WP29):[311]

> Nella realtà, i RPD realizzano l'inventario dei trattamenti e mantengono il registro di tali trattamenti sulla base delle informazioni fornite loro dai vari uffici o unità che trattano dati personali. È una prassi consolidata e fondata sulle disposizioni di numerose leggi nazionali nonché sulla normativa in materia di protezione dati applicabile alle istituzioni e agli organismi dell'UE.[312]
>
> L'articolo 39, paragrafo 1, contiene un elenco non esaustivo dei compiti affidati al RPD. Pertanto, niente vieta al titolare del trattamento o al responsabile del trattamento di affidare al RPD il compito di tenere il registro delle attività di trattamento sotto la responsabilità del titolare o del responsabile stesso. Tale registro va considerato uno degli strumenti che consentono al RPD di adempiere agli obblighi di sorveglianza del rispetto del regolamento, informazione e consulenza nei riguardi del titolare del trattamento o del responsabile del trattamento.
>
> In ogni caso, il registro la cui tenuta è obbligatoria ai sensi dell'articolo 30 deve essere considerato anche uno strumento che consente al titolare del trattamento e all'autorità di controllo, su richiesta, di disporre di un quadro complessivo dei trattamenti di dati personali svolti dallo specifico soggetto. In quanto tale, esso costituisce un presupposto indispensabile ai fini dell'osservanza delle norme e, pertanto, un'efficace misura di responsabilizzazione.

Per un nuovo RPD, ciò richiede, prima di tutto (la supervisione del-) la creazione di un **inventario** di tutte le attività di trattamento potenzialmente concernenti dati personali effettuate dall'organizzazione e dei suoi legami con altre organizzazioni. A tale scopo occorre individuare quali dati siano "personali", il che non è sempre di immediata definizione.[313]

Un **inventario iniziale ed essenziale** può utilmente essere predisposto parallelamente alla più ampia definizione delle attività dell'organizzazione e del suo contesto operativo, nel quadro del compito preliminare (Compito 0), sopra descritto. Fatta salva l'esenzione, sopra ricordata, esso dovrebbe essere poi seguito da un **inventario completo.**

L'**inventario completo** dovrebbe portare alla creazione di un **registro** (la raccolta dei "**record**") di tutte le attività di trattamento menzionate nell'art. 30 (vedi *infra:* "*Contenuti e struttura delle voci del registro*"), che dovrebbe da quel momento in poi (e dopo la revisione e la verifica, vedi *infra,* Compiti 2 e 3) essere mantenuto aggiornato dal RPD: si veda *infra,* "*Monitoraggio continuativo della conformità*").

Esenzione:

L'art. 30, paragrafo 5 esonera **le imprese o organizzazioni con meno di 250 dipendenti, e che trattano dati personali solo occasionalmente**, dall'obbligo di mantenere un registro delle attività di trattamento di dati. Tuttavia, tale eccezione non si applica se:

---

311 Gruppo art. 29, Linee-guida sui responsabili della protezione dei dati (RPD), WP243 rev 1 (vedi nota 239, *supra*), sezione 4.5, p. 18.

312 Art. 24, paragrafo 1, lett. d) del Regolamento (CE) 45/2001

313 V. WP29, Parere 4/2007 sul concetto di dato personale (WP136), adottato il 20 giugno 2007, disponibile qui: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

- il trattamento che esse effettuano può "presentare **un rischio per i diritti e le libertà dell'interessato**" (si noti che non deve necessariamente trattarsi di un "rischio elevato", che implica la necessità di effettuare una valutazione di impatto sulla protezione dei dati - Compito 4): qualunque rischio per i diritti e le libertà degli interessati, per quanto piccolo, richiederebbe la registrazione (e revisione) delle attività del titolare;
- il trattamento **non è occasionale;** o
- il trattamento include **dati sensibili o dati relativi a condanne penali e a reati**.

Riguardo al primo punto, nel contesto della valutazione d'impatto (necessaria in presenza della probabilità di "*rischio elevato per i diritti e le libertà delle persone fisiche*": vedi *infra*, Compito 4), il Gruppo art. 29 descrive il termine "**rischio",** come[314] NOTA:

> uno scenario che descrive un evento e le sue conseguenze [negative], stimate i termini di severità e di probabilità

e spiega che

> il riferimento ai "**diritti e alle libertà**" degli interessati in primo luogo si riferisce ai diritti alla protezione dei dati e alla vita privata ma potrebbe anche coinvolgere altri diritti fondamentali quali la libertà di espressione, di pensiero, la libertà di circolazione, il divieto di discriminazione, il diritto alla libertà coscienza e religione.

Nel mese di aprile 2018, il WP29 ha prodotto un "documento di posizione" sull'Art. 30, paragrafo 5, del RGPD[315]. Nel documento si evidenzia quanto segue:

> la formulazione letterale dell'art. 30, paragrafo 5, preveda chiaramente che le tre tipologie di trattamento cui non si applica la deroga in oggetto sono reciprocamente alternative ("o"), cosicché in presenza di qualsivoglia fra esse nasce l'obbligo di tenere un registro delle attività di trattamento.
>
> Ne consegue che un titolare o un responsabile il quale, pur avendo meno di 250 dipendenti, versi in una situazione tale per cui il trattamento svolto possa presentare un rischio (si noti, non un rischio elevato) per i diritti e le libertà dell'interessato, oppure tratti dati personali in via non occasionale, oppure tratti categorie particolari di dati ai sensi dell'art. 9, paragrafo 1, o dati relativi a condanne penali e a reati di cui all'art. 10, dovrà tenere un registro delle attività di trattamento.
>
> Tuttavia, è sufficiente che questi soggetti tengano un registro delle attività di trattamento solo con riguardo alle tipologie di trattamento di cui all'art. 30, paragrafo 5.
>
> Per esempio, una piccola azienda verosimilmente tratterà su base regolare dati relativi ai dipendenti. Ne deriva che un trattamento del genere non potrà essere ritenuto "occasionale" e dovrà quindi figurare nel registro delle attività di trattamento.[316] Viceversa, altri trattamenti

[314] Gruppo art. 29, Linee-guida sulla DPIA (nota 340, *infra*), p. 6.

[315] WP29, Documento di posizione sulle deroghe all'obbligo di tenuta di registri delle attività di trattamento ai sensi dell'Art. 30, paragrafo 5, del RGPD, 19 aprile 2018, disponibile qui: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51422.

[316] Il Gruppo di lavoro "Articolo 29" ritiene che un trattamento sia da ritenersi "occasionale" se non viene condotto su base regolare e ha luogo al di fuori della normale attività imprenditoriale o di altro genere svolta

che hanno realmente carattere "occasionale" non devono figurare nel registro delle attività di trattamento, purché non possano presentare un rischio per i diritti e le libertà degli interessati e non riguardino categorie particolari di dati o dati personali relativi a condanne penali e a reati.

Esempio:

In **Croazia**, informazioni dettagliate su tutti i funzionari e i dipendenti pubblici devono essere per legge caricati su un sistema centrale, *il Registro dei dipendenti pubblici.* Tale obbligo si applica anche alle più piccole entità, come le piccole comunità locali che potrebbero avere solo pochi dipendenti. Il trattamento dei dati relativi a tali pochi dipendenti da parte di quella comunità, seppur molto piccola, è pertanto "non occasionale" e non beneficia dell'esenzione dall'obbligo di tenuta del registro.

In caso di dubbio, il titolare dovrebbe chiedere il parere del RPD su tali questioni, e l'RPD dovrebbe propendere per la creazione di un registro completo, piuttosto che rischiare che l'organizzazione sia ritenuta responsabile di non aver adempiuto agli obblighi previsti dall'art. 30, paragrafi 1-4.

Note:

1. Sulla questione se il registro delle attività di trattamento debba essere o meno accessibile a chiunque (online o attraverso altre modalità), vedi il Compito 14, "*Compiti di informazione e sensibilizzazione*".
2. La creazione del registro in sé non comporta una valutazione dell'osservanza delle attività in esso registrate al RGPD: tale valutazione è effettuata nel Compito 2 – anche se, naturalmente, il registro dovrebbe essere modificato e aggiornato se e ogni qualvolta siano apportate modifiche alle attività di trattamento in esso registrato: vedi *infra* "*Controllo della conformità: Ripetizione dei Compiti 1 – 3 (e 4) su base continuativa*).

Contenuti e struttura delle voci del registro:

Il RGPD distingue i registri del titolare da quelli del responsabile.

Contenuti e struttura delle voci del registro del titolare :

In base all'art. 30, paragrafo 1 del RGPD, il **registro** delle attività di trattamento di un *titolare* consiste in una raccolta di **informazioni** di ciascuna attività di trattamento; e **ciascuna raccolta deve includere le seguenti informazioni** (parole in parentesi quadra e corsivo sono qui aggiunti):

a. il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
b. le finalità del trattamento;

dal titolare o dal responsabile. Si vedano le Linee-guida del Gruppo "Articolo 29" sull'art. 49 del Regolamento 2016/679 (WP262).

c. una descrizione delle categorie di interessati e delle categorie di dati personali; [*compreso se vi sono dati che ricadono nella lista delle "categorie particolari di dati personali"/dati sensibili*];

d. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e. ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

f. ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Questa lista non ricomprende la **base giuridica** del trattamento dei dati in questione (Articolo 6 per i dati non sensibili; Articolo 9 per quelli sensibili) né gli strumenti giuridici utilizzati per stipulare contratti con responsabili del trattamento, o ai fini dei trasferimenti di dati, ma si tratta di aspetti talmente cruciali al fine di determinare la legittimità e la compatibilità con il RGPD di qualunque trattamento, che anch'essi dovrebbero figurare nel registro, con riferimento a ciascuna attività di trattamento (definita con riferimento alla finalità del trattamento stesso) – avendo verificato a tempo debito la validità della base giuridica dichiarata e riportata [nel registro].

MODELLO BASE DI REGISTRO DELLE ATTIVITA' DI TRATTAMENTO DEL TITOLARE

Si noti che per ciascun trattamento occorre creare una voce separata

Parte 1 – Informazioni sul titolare, ecc.

DATI DI CONTATTO DEL **TITOLARE**:	Nome, indirizzo, email, telefono
DATI DI CONTATTO DEL **CONTITOLARE**:*	Nome, indirizzo, email, telefono
DATI DI CONTATTO DEL **RAPPRESENTANTE**:*	Nome, indirizzo, email, telefono
(*) ***se applicabile***	
DATI DI CONTATTO DEL **RPD**:	Nome, indirizzo, email, telefono

Parte 2 – Informazioni essenziali sull'attività di trattamento[317]

[317] La tabella qui sopra intende semplicemente illustrare in termini generali i requisiti della registrazione. Il **modello dettagliato di registro** menzionato nella precedente nota e allegato a questo Compito richiede maggiori dettagli, ad esempio, per ciascuna categoria di dato personale: la finalità, la rilevanza, l'origine dei dati, ecc..

1. Denominazione dell'attività di trattamento [318]	
2. Responsabile dell'unità ("referente")	
3. Finalità dell'attività di trattamento	
4. Categorie di interessati	
5. Categorie di dati	
6. Sono previsti dati sensibili?	
7. Base legale per il trattamento:* * Cf. Art. 6 RGPD per dati non sensibili, Art. 9 per dati sensibili	
8. I dati sono trasferiti verso un Paese terzo o un'organizzazione internazionale?	
9. In caso di trasferimenti previsti dal secondo capoverso dell'art. 49, paragrafo 1, del RGPD: quali sono le garanzie adeguate previste?	
10. Limiti temporali per la cancellazione	
11. Dettagli delle applicazioni dei sistemi e dei trattamenti (*file* elettronici/su carta; software locale/centralizzato/servizi cloud /rete locale; trasmissione dei dati; etc.) e le relative misure (di sicurezza) tecniche e organizzative	
12. Il trattamento comporta l'utilizzo di uno o più responsabili del trattamento? In caso	

[318] Dal punto di vista della protezione dei dati, qualunque attività di trattamento è meglio definita sulla base della finalità perseguita dal trattamento (come riportato al 2). Tuttavia, in molte organizzazioni, le persone che effettuano il trattamento, avranno spesso una denominazione interna/funzionale specifica per tale attività, nonostante le due designazioni possano essere ovviamente sovrapposte se non identiche.

affermativo inserire tutte le informazioni pertinenti e copia dei relativi contratti.	

Contenuti e struttura delle voci del registro del responsabile[319]

In base all'articolo 30, paragrafo 2 del RGPD, il **registro** delle attività di trattamento di un *responsabile* consiste nella raccolta di **records** di ciascuna attività; e ciascuno di tale **record deve includere le seguenti informazioni**:

a. il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;

b. le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c. ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

d. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Di seguito, riproporremo di nuovo un modello di registro che un responsabile dovrebbe tenere per rispettare tali requisiti.

MODELLO DI REGISTRO DI TRATTAMENTO DI DATI PERSONALI DEL RESPONSABILE[320]

Si noti che per ciascun trattamento occorre creare una voce separata per ciascun titolare

Parte 1 – Informazioni sul responsabile e altro/i responsabile/i [cui ricorre il responsabile del trattamento per l'esecuzione di specifiche attività di trattamento], cd. sub-responsabile/i

DATI DI CONTATTO DEL **RESPONSABILE**:	Nome indirizzo, email, telefono
DATI DI CONTATTO DEL **RPD**:	Nome indirizzo, email, telefono

[319] Si noti che è sempre più difficile distinguere chiaramente i titolari dai responsabili. Spesso, le entità che erano solite fornire servizi chiaramente definibili "da responsabile" (e che agivano cioè esclusivamente secondo le istruzioni del titolare che ne determinava i mezzi e le finalità) assumono ora molte più responsabilità e possono diventare "contitolari". Ciò è particolarmente vero in relazione ai fornitori di servizi cloud, alcuni dei quali offrono persino "Intelligenza artificiale e apprendimento automatico (AI / ML) tramite Machine-Learning-as-a-Service (MLaaS)", vedi:
http://www.techmarketview.com/research/archive/2018/04/30/machine-learning-as-a-service-market-overview-technology-prospects
Come sottolineato nel *Compito preliminare*, gli accordi tra entità coinvolte in queste complesse relazioni dovrebbero essere opportunamente e chiaramente registrati. I modelli che registrano le relative attività di trattamento dovrebbero essere rivisti e modificati per adattarsi a questi accordi tra entità.

[320] Anche questo modello è sviluppato a partire da quello presentato da Carrozzi (v. nota 233, *supra*) con modifiche.

DATI DI CONTATTO DEL **SUB-RESPONSABILE**:*	Nome indirizzo, email, telefono
DATI DI CONTATTO DEL **RPD**:	Nome indirizzo, email, telefono
DATI DI CONTATTO DEL **SUB-RESPONSABILE**:*	Nome indirizzo, email, telefono
DATI DI CONTATTO DEL **RPD**:	Nome indirizzo, email, telefono

** Se applicabile*

Parte 2 – Informazioni sul titolare della specifica attività di trattamento

DATI DI CONTATTO DEL **TITOLARE**:	Nome indirizzo, email, telefono
DATI DI CONTATTO DEL **CONTITOLARE**:*	Nome indirizzo, email, telefono
DATI DI CONTATTO DEL **RAPPRESENTANTE:***	Nome indirizzo, email, telefono
(*) *Se applicabile*	
DATI DI CONTATTO DEL **RPD**:	Nome indirizzo, email, telefono

NB: Il rapporto tra titolare e responsabile e tra responsabile e qualunque sub-responsabile, deve essere basato su un contratto scritto che risponda ai requisiti di cui all'art.28 del RGPD. I responsabili dovrebbero conservare copia dei contratti in questione con la sezione del registro compilata come sopra.

Parte 3 – Descrizione dettagliata dell'attività di trattamento

1. La tipologia di trattamento effettuato per il titolare in rapporto all'intero trattamento, inclusi:	
- Le categorie degli interessati;	
- Le categorie di dati personali; e	
- Se sono inclusi anche dati sensibili.	
2. I dati vengono trasferiti verso un Paese terzo o un'organizzazione internazionale?	
3. In caso di trasferimento ai sensi del secondo capoverso dell'art. 49, paragrafo 1 del RGPD: quali sono le garanzie adeguate fornite?	
4. Dettagli dei sistemi, delle applicazioni e dei trattamenti utilizzati (*file* elettronici/su carta; software locale/centralizzato/servizi cloud /rete locale; trasmissione dei dati; etc.) e relative misure tecniche e	

	organizzative (di sicurezza)	
5.	Il trattamento comporta il ricorso a sub-responsabili del trattamento? In caso affermativo, fornire tutte le informazioni pertinenti e copia dei relativi contratti.	

Contenuti e struttura del registro:

Il RPD dovrebbe costruire il **registro** sulla base delle informazioni che riceve su ogni distinta attività di trattamento. Di norma è preferibile ordinare le informazioni per ente (che procede al trattamento) e, all'interno di tale ente, per singolo referente di attività. Il RPD dovrebbe conservare tutta la documentazione pertinente per ogni voce (come sopra indicato).

Il RPD dovrebbe annotare nel registro quando ciascuna informazione è stata ricevuta, quando si è proceduto all'esame del singolo trattamento (vedi Compito 2, *infra*), e l'esito di tale esame, nonché ogni misura correttiva adottata; e indicare quando è previsto il successivo esame del trattamento (per es. a distanza di un anno).

- o – O – o –

Allegato: Modello di descrizione dettagliata di trattamento del dati personali[321]

[321] Un modello di registrazione di dati personali più dettagliato è anche previsto dall'Autorità polacca, *Urząd Ochrony Danych Osobowych* (UODO) reperibile sul suo sito web, in lingua polacca, al seguente link: https://uodo.gov.pl/pl/123/214 (si segua il primo link alla fine della pagina).

Allegato:

MODELLO DI DESCRIZIONE DETTAGLIATA DEL TRATTAMENTO DI DATI PERSONALI

Si prega di utilizzare un modulo separato per ciascuna distinta attività di trattamento dati.

NB: Se avverte la necessità di elaborare o chiarire una questione, si prega di allegare, con un opportuno richiamo, una pagina contenente tali elaborazioni o chiarimenti.

I. GENERALE: * indica un campo obbligatorio (se applicabile)

Titolare: (Principale titolare)* (Nome, luogo di stabilimento e indirizzo, numero di registrazione, ecc.)	
Soggetti associati nel trattamento (qualunque soggetto cui il titolare è legato in relazione a questa attività di trattamento, ad es. società madre e figlia, o enti pubblici collegati; responsabili coinvolti)	
Unità responsabile: ("Referente dell'attività")* (ad es. Risorse umane, Contabilità, Ricerca e sviluppo, Vendite, Assistenza ai clienti)	
Referente all'interno dell'unità	
PRINCIPALE FINALITA' DELL'ATTIVITA' DI TRATTAMENTO:* ***Si prega di specificare nella maniera più precisa possibile***	
I dati personali sono utilizzati o comunicati per qualunque altra/e finalità (secondaria/e)? * ***Si prega di specificare nella maniera più precisa possibile e di aggiungere un link o un riferimento al record associato.***	
Questa attività di trattamento è effettuata allo stesso modo per tutte le entità associate? O separatamente e/o differentemente per diverse entità?* ***Si prega di specificare.*** ***Se le operazioni sono differenti per le diverse entità, si prega di utilizzare moduli separati per ciascuna di esse.***	

Approssimativamente, a quanti individui (interessati) si riferisce questo trattamento (se conosciuto)?*	[*Aggiungere il numero o la dicitura "non noto"*]
Data di presentazione di questo modulo al RPD*	
Modulo e attività di trattamento rivista dal RPD:	[*Sì/No e data, che deve essere aggiunta dal RPD*]
Data prevista per revisione/aggiornamento di questo modulo:	[*Specificazione da parte del RPD*]

II. INFORMAZIONI SULL'ATTIVITA' DI TRATTAMENTO DI DATI PERSONALI:

II.1 I dati e la loro origine [NB: ove applicabile, tutti i campi sono obbligatori, a meno che non sia altrimenti indicato]

1. Quali dati personali o categorie di dati personali sono raccolti ed utilizzati per questa operazione?	*Indicare √ se appropriato:*	**Quando, come e da chi sono ottenuti tali dati?** **Ad es.:** (interessato) - Dal Ministero del lavoro, al momento dell'assunzione - Dall'interessato, al momento dell'inserimento nella ricerca
- Cognome/I e Nome/i)		
- Data di nascita		
- Indirizzo abitazione		
- Numero di telefono lavoro		
- Numero di telefono privato		
- Indirizza di posta elettronica lavoro		
- Indirizza di posta elettronica personale		
Se applicabile, si aggiunga qui sotto qualsiasi altro dato:* ** sI veda anche sotto, punto 2, in materia di dati sensibili*		
Si aggiungano ulteriori righe se necessario		
2. I dati da lei raccolti e registrati per l'attività di trattamento <u>includono o indirettamente rivelano</u> alcuna delle seguenti	*Indicare √ se i dati sono espressamente raccolti ed utilizzati per l'operazione;* *Indicare √ e aggiungere ("Indiretto") se il dato è*	**Quando e da chi sono ottenuti i dati?** **Ad es.:** (interessato= I)

categorie particolari di dati personali ("dati sensibili")?	*indirettamente rivelato (spiegare in una nota se necessario)*	- Dal Ministero del lavoro, al momento dell'assunzione - Dall'interessato, al momento dell'inserimento nella ricerca
- Origine razziale o etnica		
- Opinioni politiche o affiliazioni		
- Convinzioni religiose o filosofiche		
- Appartenenza a sindacato		
- Dati genetici		
- Dati biometrici		
- Dati relative alla salute della persona		
- Dati relativi all'orientamento o la vita sessuale di una persona		
- Informazioni su condanne penali o reati		
- Identificativo nazionale * * ad es., Codice fiscale		
- Dati relative all'affidabilità creditizia		
- Dati sui minori		
3. Se conosciuto o deteminato: per quanto tempo sono conservati i dati (particolari e gli altri)? Cosa succede al termine della conservazione?* * Indicare periodo o evento, ad es. "7 anni" o "fino a 5 anni dal termine del rapporto lavorativo". Si spieghi anche cosa avviene ai dati, ad es. cancellazione/distruzione, o trasformazione in forma anonima. **NB: Si prega di indicare se ci sono differenti periodi di conservazione per diversi dati.**		

II.2 Comunicazione di dati

4. A quali terze parti vengono comunicati i dati? E per quali finalità? **NB: Ciò si applica anche ai dati che sono resi accessibili, specialmente direttamente, on line. Sulla divulgazione che comporta trasferimento verso paesi terzi, si veda sotto, punto II. 5**	**Terza parte destinataria e luogo e Paese di stabilimento:**	**La/le finalità della/e divulgazione/i:**

TUTTI I DATI INDICATI NELLA SEZIONE II.1		
***o:* i seguenti dati** (Copiare i dati da 1 e 2, sopra)		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
Aggiungere ulteriori righe se necessario		

II.3 Base giuridica del trattamento

5. **Su quale base giuridica avviene il trattamento ?** **NB: <u>Si prega di indicare se vi sono differenti basi giuridiche per diversi dati o per diverse finalità (primarie, secondarie o nuove, non collegate) (se necessario copiando le liste dei dati da sopra a sotto, e spostando le differenti basi giuridiche nella seconda colonna)</u>**	*Indicare la base giuridica rilevante e fornire chiarimenti nella successiva colonna se pertinente.*	**Chiarimenti:**
- L'interessato ha acconsentito al trattamento		

NB: Si veda anche Domande 6 – 9, sotto.		
- Il trattamento è necessario [per l'esecuzione] del contratto tra la tua organizzazione e l'interessato (O al fine di prendere iniziative, su richiesta dell'interessato, precedenti alla stipula di un contratto – ad es. ottenere referenze)		
- il trattamento è necessario per adempiere ad un obbligo legale al quale la tua organizzazione è soggetta * ad es. nell'ambito del diritto del lavoro o degli obblighi fiscali – *si prega di specificare la normativa in questione*		
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica		
- il trattamento è necessario per l'esecuzione di un compito di interesse pubblico * * *Si prega di specificarne la fonte (tipicamente una norma di legge)*		
- il trattamento è connesso all'esercizio di pubblici poteri * *Si prega di specificarne la fonte (tipicamente una norma di legge)*		
- il trattamento è necessario per il perseguimento del legittimo interesse della tua organizzazione (o di un'altra entità) e non prevalgano gli interessi degli interessati Ad es. marketing verso i propri clienti, o prevenzione delle frodi – si prega di specificare.		

CONSENSO – ulteriori dettagli:	
6. **se i dati sono trattati sulla base del consenso degli interessati, quando e come è ottenuto tale consenso?** **NB: Se il consenso è fornito su format elettronico o cartaceo, si prega di fornire una copia del testo/link rilevante**	
7. Quale prova del prestato consenso è conservata? Ad es. sono conservate copie dei moduli cartacei, o I log del consenso elettronico?	
8. Per quanto tempo la prova è conservata?	
9. Se nell'ambito di un contratto sono chiesti dalla tua organizzazione più dati di quanto non sia necessario per il contratto, l'interessato è messo a conoscenza del fatto che non è tenuto/a a fornire ulteriori dati? **NB: Si dica "Non Applicabile", o, ove applicabile, fornire una copia del testo/link rilevante**	

II.4 Informativa agli interessati [NB: questa informazione non è obbligatoria ma è tuttavia utile nella verifica e revisione delle politiche interne di protezione dati]

10. **Gli interessati sono informati dei seguenti elementi? E se sì, quando e come?**	*Indicare Sì/No (o "Non applicabile.")* **NB: se rilevante, puoi specificare che "Appare ovvio nel contesto" e/o "L'interessato ha già avuto tali informazioni"**	Spiega come e quando ciò viene fatto **Si prega di fornire copia di qualsiasi informativa o link**
- Che la tua organizzazione è titolare del trattamento di dati personali?		
- Dettagli sulla tua organizzazione (ad es. nome e numero di registrazione)?		

- Ove applicabile, dettagli sul tuo rappresentante in EU?		
- I dati di contatto del RPD?		
- La finalità principale del trattamento?		
- Qualunque finalità ulteriore per cui la tua organizzazione vuole (o potrebbe volere) trattare i dati?		
- Se i dati non sono stati ottenuti direttamente dagli interessati, l'origine o le origini di tali dati, e se esse includevano anche fonti pubblicamente accessibili (come i pubblici registri)?		
- I destinatari o le categorie di destinatari dei dati? **NB: Cfr. Domanda 4, sopra**		
- Se i dati sono (o devono essere) trasferiti verso un paese extra UE/AEE (ad es. verso un fornitore cloud negli Stati Uniti)? **NB: Ciò si applica ai dati resi accessibili (specialmente in maniera diretta, on line) alle entità in stati extra UE/AEE.**		
- Se i dati sono trasferiti, quali garanzie sono state poste in essere e dove gli interessati possono ottenerne copia? **NB: Le garanzie possono essere previste nei contratti per il trasferimento dei dati o attraverso codici di condotta o certificazioni**		
- Per quanto tempo i dati saranno conservati?		
- Diritto di accesso, rettifica, cancellazione, limitazione, opposizione?		
- Diritto di presentare reclamo alla competente		

autorità di protezione dati?		
11. Se tutti o parte dei dati sono trattati sulla base del consenso, gli interessati sono informati dei seguenti elementi?		
- Del loro diritto di revocare il proprio consenso in qualunque momento (e delle modalità per farlo) (senza che ciò infici la liceità del pregresso trattamento)?		
12. Se la cessione dei dati è prevista da contratto o obblighi di legge (o è condizione per la stipula di un contratto), gli interessati sono informati dei seguenti elementi?	*Indicare Sì/No (or "Non applicabile")* **NB: Se pertinente, si può dire "appare ovvio nel contesto" e/o "l'interessato ha già tale informazione"**	Spiegare quando e come ciò viene fatto **Si prega di fornire copia di qualunque informativa o link**
- Se sono tenuti a fornire i dati e le conseguenze in caso ciò non avvenga?		
13. **Se tutti o parte dei dati sono trattati sulla base del criterio del "legittimo interesse" gli interessati sono informati su quale sia tale legittimo interesse?**		Si prega di fornire una breve sintesi dei criteri applicati nel bilanciamento effettuato con riferimento ai diritti fondamentali e le libertà degli interessati, così come previsto dall'art. 6, paragrafo 1, lett.f) del RGPD.
14. **Se gli interessati saranno sottoposti a decisioni automatizzate o profilazione, sono informati dei seguenti elementi ?**		Si prega di fornire una breve sintesi della logica utilizzata nella decisione automatizzata o profilazione.
- Che tale decisione automatizzata o profilazione sarà posta in essere?		
- In termini generali (ma significativi), quale sia la "logica" del trattamento?		
- Quale sia il significato della decisione		

automatizzata o della profilazione e le loro conseguenze previste?		

II.5 Trasferimenti di dati [NB: Una voce nel campo 17 non è obbligatoria, ma è utile per la valutazione interna]

15. **Ci sono dati che vengono trasferiti verso paesi terzi [extra UE/SEE] o organizzazioni internazionali che non sono stati ritenuti in grado di offrire un livello adeguato di protezione ai sensi dell'art. 45 del RGPD?**	*Indicare Sì/No e il/i paese/i in questione.* *Se il trasferimento si riferisce solamente ad alcuni ma non a tutti i dati, specificare per ciascuna delle categorie di dati.*	*Spiegare la finalità del trasferimento, in quanto parte dei trattamenti della tua organizzazione (ad es. nell'utilizzo di software cloud e.g), o della comunicazione dei dati a una terza parte (si prega di specificare tale/i parte/i)*
TUTTI I DATI ENUMERATI NELLA SEZIONE II.1		
***O:* I seguenti dati:** (Copiare i dati da 1 e 2, sopra)		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
Aggiungere ulteriori righe se necessario		

16. **Ci sono dati che vengono trasferiti verso paesi terzi [extra UE/SEE] o organizzazioni**	*Indicare Sì/No e il/i paese/i in questione.* *Se il trasferimento si riferisce solamente*	*Spiegare la finalità del trasferimento, in quanto parte dei trattamenti della tua organizzazione (ad es.*	*Quale salvaguardia o deroga è alla*

internazionali che non sono stati ritenuti in grado di offrire un livello adeguato di protezione ai sensi dell'art. 45 del RGPD?	*ad alcuni ma non a tutti i dati, specificare per ciascuna delle categorie di dati*	*nell'utilizzo di software cloud), o della comunicazione dei dati a una terza parte (si prega di specificare tale/i parte/i)*	*base del trasferimento?* *Si prega di fornire un numero come da elenco nella *Nota di seguito e una copia di ogni documento pertinente*
NB: *Se I dati sono trasferiti per finalità differenti verso diversi destinatari in diversi paesi, si prega di rispondere alle domande separatamente per ogni trasferimento.*			
TUTTI I DATI ENUMERATI NELLA SEZIONE II.1			
O: i seguenti dati: (Copiare i dati da 1 e 2, sopra)			
-			
-			
-			
-			
-			
-			
-			
Aggiungere ulteriori righe se necessario			

*** NOTA:** In base al RGPD, i trasferimenti verso Paesi che si considerano non "adeguati" possono avvenire solamente se sono poste in essere "garanzie adeguate", così come enumerate nella colonna di sinistra in fondo, o se si applica una deroga, così come enumerata nella colonna di destra.

Garanzie ai sensi dell'art. 46 del RGPD : 1. Strumento internazionale [giuridicamente vincolante] tra autorità pubbliche; 2. Norme vincolanti d'impresa (Binding Corporate Rules - BCRs); 3. Clausole tipo di protezione dati adottate; 4. Codice di condotta; 5. Certificazione; 6. Clausole ad hoc adottate	Le deroghe previste dall'art. 49 del RGPD, ove non siano applicabili le salvaguardie di cui all'art. 46 (a tal proposito si vedano le linee-guida del Board per le quali applicazione e interpretazione delle deroghe devono essere restrittive): 7. Consenso; 8. Contratto tra titolare e interessato 9. Contratto tra titolare e una terza parte 10. Necessità [del trasferimento] per importanti motivi di interesse pubblico 11. Necessità [del trasferimento] per esercizio di un diritto in giudizio; 12. Necessità [del trasferimento] per tutelare gli interessi vitali dell'interessato o di altre persone;

	13. Il trasferimento sia effettuato a partire da un registro accessibile al pubblico
17. Esistono regole in relazione a eventuali sentenze di organi giurisdizionali e/o decisioni di un'autorità amministrativa di un paese terzo, notificate al titolare o a un responsabile, che impongano al titolare o al responsabile di trasferire o divulgare i dati personali? (Cfr. Art. 48 RGPD)	*Indicare Sì/No e se sì, si prega di fornire una copia di tali norme.*

III. SICUREZZA E RISERVATEZZA

NB: Se le risposte alle domande sottostanti differiscono per i diversi dati, si prega di rispondere separatamente per ogni distinto insieme di dati.	*Si prega di fornire dettagli:*
I dati personali elencati al punto II.1 sono conservati su supporto cartaceo o elettronico? Se su carta, sono contenuti in una raccolta manuale strutturata (archivio di dati)?	
Dove sono (fisicamente) memorizzati i dati? (Nei vostri uffici? Sui server del titolare principale? Sui server di un'organizzazione collegata? Sui server di una terza parte (ad esempio, un fornitore di servizi cloud)?	
Quali misure sono in atto per proteggere da accessi non autorizzati ai luoghi fisici in cui i dati sono archiviati/accessibili? Esiste una politica di sicurezza dei dati che regola tale aspetto? (*In tal caso, si prega di fornirne copia.)*	

Quale hardware viene utilizzato nel trattamento dei dati? Chi è responsabile della gestione e della sicurezza di questo hardware?	
I dati sono memorizzati su supporti / dispositivi rimovibili? Di che supporti/dispositivi si tratta? Chi li detiene?	
Le persone che hanno accesso ai dati possono utilizzare i dispositivi personali per accedere o elaborare i dati? In tal caso, esiste una policy BYOD (Bring your own device) su questo? *Si prega di fornirne copia*	
Le persone autorizzate ad accedere ai dati personali sono soggette ad un obbligo di riservatezza (che si tratti di un obbligo di legge, o di regole professionali o di previsioni contrattuali)? Si prega di fornire dettagli o copie di eventuali norme pertinenti o clausole contrattuali.	
Quale/i software / applicazioni è/sono utilizzato/i nell'elaborazione dei dati? (Ad es. suite MS Office per desktop, applicazione gestita centralmente, servizio cloud, ecc.)	
Questo software è gestito localmente o centralmente? Se centralmente, chi è l'entità centrale? Se non sei tu, c'è un accordo formale tra quell'entità e la tua organizzazione riguardo l'uso del software? *Si prega di fornire una copia di tale accordo.*	
- Il software utilizza un "cloud"? In tal caso, chi è il fornitore di servizi cloud e dove è stabilito giuridicamente quel fornitore? E dove è/sono fisicamente stabilito/i il server/i cloud? I dati sul server cloud sono completamente crittografati? In che modo (cioè, utilizzando quale tecnologia di	

crittografia)? *Si prega di fornire una copia del contratto in base al quale questo trattamento è effettuato.*	
- Chi è responsabile (chi ha l'autorità di "amministrare") per questo software? (Lei? Qualcun altro all'interno della organizzazione? Qualcuno in una entità centrale con la quale si è collegati? Altri soggetti?)	
I dati in qualunque momento/circostanza sono trasmessi elettronicamente ad altro sistema o dispositivo?	
Se sono trasmessi elettronicamente, ciò viene fatto: - su Internet? Se sì, i dati sono criptati? Come (ad es. attraverso l'uso di crittografia)? - attraverso File Transfer Protocol (FTP)? Come è garantita la sicurezza? - Attraverso una VPN (rete privata virtuale)? Come è garantita la sicurezza? - altro – *si prega di specificare*	

- o – O – o -

COMPITO 2: Riesame delle attività di trattamento di dati personali

Dopo aver creato il registro delle attività di trattamento della sua organizzazione (Compito 1), il passo successivo per il RPD consiste nell'eseguire una revisione approfondita di tutte le attività di trattamento dei dati personali registrate, per verificare se soddisfano i requisiti del RGPD in tutti gli aspetti rilevanti, anche in relazione a:

- principio di finalità e necessità;
- la validità di qualunque consenso prestato (e l'esistenza di prove documentali dell'avvenuta prestazione del consenso) o applicabilità di altra base giuridica per il trattamento;
- dati personali trattati e la loro rilevanza e necessità in relazione alle specifiche finalità del trattamento
- qualità dei dati (accuratezza, attualità, ecc., nonché minimizzazione dei dati e pseudonimizzazione);
- informazioni fornite all'interessato di propria iniziativa (sia quando i dati sono raccolti presso l'interessato o altrimenti, o su richiesta - anche in relazione ai dati raccolti dai visitatori del sito Web);
- il periodo di tempo in cui i dati sono conservati in forma identificabile e ogni informazione relativa a meccanismi di deidentificazione;
- sicurezza dei dati tecnica, organizzativa e fisica (inclusi limiti di accesso fisico e limitazioni tecniche di accesso [nome utente, password, politiche PIN, ecc.], crittografia, ecc.);
- trasferimenti di dati transfrontalieri (e le relative previsioni normative o altre disposizioni contrattuali o di altro tipo);
- eccetera.

Alla luce delle conclusioni raggiunte sulla base degli elementi di cui sopra, l'RPD dovrebbe essere in grado infine di **valutare**:

- se il trattamento nel suo insieme può essere considerato conforme al principio imperativo di liceità e correttezza.

(Si noti che questa valutazione della conformità al RGPD è separata e diversa dalla valutazione del rischio, descritta di seguito come Compito 3).

I record delle singole attività di trattamento creati nel Compito 1 (in particolare se creati nel formato più dettagliato) dovrebbero costituire la base della revisione, in quanto porteranno il RPD a chiedere e rispondere a domande pertinenti, tra cui, in particolare:

- è sufficientemente chiaro quale entità è il **titolare** del trattamento dei dati personali, e se sono coinvolte altre entità, qual è il loro rispettivo ruolo (ad esempio, **contitolare**,

responsabile, o altro titolare di terze parti)? Se questo non è ovvio, vi sono **accordi formali** che chiariscono questi aspetti (cfr. Compito 1, sopra)?

- È sufficientemente chiaro quale unità aziendale è il "**referente**" in relazione al trattamento dei dati (ad es., che ha di fatto una responsabilità quotidiana *de facto* del trattamento)? Questo è descritto in un documento formale (ad es., istruzioni specifiche dal titolare all'unità)?
- La o le **finalità** del trattamento dei dati personali è/sono specificata/e in termini sufficientemente precisi? Dove (ad es., in che tipo di **documento**)? Se i dati personali trattati vengono utilizzati per più di uno scopo, qual è la **finalità principale del trattamento** e quali le **finalità secondarie**? Questi scopi secondari sono **compatibili** con lo scopo principale o sono finalità separate?
- NB: Nel valutare la compatibilità di qualsiasi trattamento per uno scopo secondario con lo scopo principale, il RPD deve tenere conto delle questioni elencate all'articolo 6, paragrafo 4, del RGPD.
- Tutte le finalità per le quali i dati personali sono trattati sono pienamente giustificate e legittime?
- I dati personali trattati sono **adeguati, pertinenti e necessari** per la <u>finalità principale</u>? Come è garantito che siano e rimangano **precisi e aggiornati** per questo scopo, e quali misure sono adottate per garantire ciò e per **rettificare** o **aggiornare** o **cancellare** informazioni inaccurate o non aggiornate?
- Le misure adottate sono adeguate e sufficienti? Sarebbe possibile raggiungere lo stesso scopo con meno rischi per la privacy e gli altri diritti delle persone interessate?
- Quali dati personali vengono utilizzati o comunicati per <u>finalità secondarie</u> o in effetti <u>nuove, non correlate</u> (in genere a terzi)? I dati personali trattati sono **adeguati, pertinenti e necessari** per tali finalità <u>secondarie o nuove, non correlate</u>? (Se tutti i dati raccolti per una finalità [primaria] sono comunicati in modo precipitoso per una/qualsiasi finalità secondaria o nuova o indipendente, essi, o alcuni di essi, potrebbero essere eccessivi per la/le finalità secondaria/e o non correlata/e. È stato considerato?)

  NB: Cfr. il modulo dettagliato di trattamento dei dati personali, al punto II.2.
- Tutte le finalità secondarie per le quali i dati personali sono trattati sono pienamente giustificate e legittime?

  - Come è garantito che i dati utilizzati o comunicati per finalità <u>secondarie o nuove, non correlate</u> siano **accurati** e **aggiornati** per quegli scopi secondari o nuovi al momento del primo utilizzo o divulgazione a tali finalità, e quali misure sono adottate per assicurarsi che *rimangano* **precisi** e **aggiornati** dopo quel primo utilizzo o divulgazione, e siano **rettificati, aggiornati o cancellati** quando diventano inaccurati o non aggiornati? Le misure in questione sono adeguate e sufficienti?

  NB: Se i dati vengono utilizzati o comunicati per più di una finalità secondaria o nuova, è necessario rispondere a queste domande separatamente per ogni singola finalità o nuovo uso o comunicazione.

- **Quando, come, da chi e in quale forma** vengono ottenuti i dati personali? Ad es.: l'interessato, un dipartimento governativo, un (ex) datore di lavoro, ecc., su carta, tramite trasferimento elettronico, ecc.
- **NB**: a questa domanda occorrerebbe dare risposta sia con riferimento ai dati **non sensibili** sia a quelli **sensibili;** occorrerebbe inoltre indicare se dati diversi sono ottenuti da fonti diverse, questo dovrebbe essere indicato. Cfr. il modulo dettagliato di trattamento dei dati personali, ai punti II.1 e II.2.

  Queste fonti sono appropriate? Alcuni dati ottenuti da terzi potrebbero forse essere meglio richiesti agli stessi interessati?
- **Per quanto tempo** sono **conservati** i dati personali (non sensibili e sensibili)? **Cosa succede alla fine di quel periodo?** (ad es.: **cancellazione, distruzione, anonimizzazione** dei dati - o **pseudonimizzazione** - ma nota che quest'ultima significa che i dati sono ancora conservati in forma identificabile)[322]. Se i dati sono conservati in forma anonima o pseudonima, **perché** viene fatto? (Ad es., per scopi di ricerca o storici? In tal caso, il trattamento per tale finalità dovrebbe essere valutato separatamente per la compatibilità con il RGPD.)
- **NB**: il periodo di conservazione può essere specificato come un tempo specifico o come un evento, ad esempio "7 anni" o "fino a 5 anni dopo la cessazione del rapporto di lavoro". Si noti che esistono **standard formali** sui metodi raccomandati per la cancellazione/distruzione per diverse categorie di dati e supporti di dati[323]. Il RPD deve verificare se sono stati seguiti (in particolare per quanto riguarda le informazioni sensibili nel senso giuridico della protezione dei dati o in un più ampio senso sociale o politico).

---

322 Si noti che ai sensi del RGPD (come previsto dalla Direttiva 95/46) si può affermare che i dati personali sono stati resi anonimi se non possono più essere collegati a un individuo specifico da *chiunque* - cioè, non solo dal titolare, ma anche, per esempio, da colleghi, parenti o amici che potrebbero conoscere i dati una volta resi disponibili via Internet o altrimenti, in un formato teoricamente anonimizzato. A tal riguardo, i RPD dovrebbero essere consapevoli del fatto che sempre più dati che potrebbero sembrare "non personali" o essere qualificati come "resi anonimi" possono essere facilmente (ri) collegati ad individui specifici. In particolare, le informazioni contenute in insiemi di dati che si presumono "anonimi" nell'ambito di Big Data sono spesso passibili di re-identificazione, al di là di quanto ipotizzabile, soprattutto se i diversi dataset sono collegati o "incrociati". Inoltre, se vengono utilizzati set di dati che non sono realmente personali per creare "profili" (siano quelli tipici dei consumatori di un particolare prodotto, o tipici pazienti, o tipici criminali o terroristi), e tali profili vengono poi applicati ai set di dati per individuare singoli individui che soddisfano il profilo – allora anche quel trattamento può incidere molto seriamente su quegli individui, a cui può essere negata l'assicurazione, o un lavoro, o l'accesso a un volo o persino a un paese (o peggio) sulla base di algoritmi di fatto non sindacabili. Vedi: Douwe Korff e Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards, Rapporto per il Comitato consultivo del Consiglio d'Europa sulla protezione dei dati, giugno 2015, documento T-PD (2015) 11, sezione I.iii, disponibili all'indirizzo: https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2015)11_PNR%20draft%20report%20Douwe%20Korff%20&%20Marie%20Georges_15%2006%202015.pdf

323 Si veda ad esempio:

- DIN German Institute for Standardization, Office machines - Destruction of data carriers, DIN 66399, ottobre 2012.
- NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization, dicembre 2014, http://dx.doi.org/10.6028/NIST.SP.800-88r1
- US National Security Agency/Central Security Service, Media Destruction Guidance, https://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml

I periodi di conservazione dei dati sono appropriati? O troppo lunghi? Le misure di cancellazione/distruzione dei dati sono conformi agli standard nazionali e internazionali? Se i dati vengono conservati oltre i normali periodi di conservazione in forma anonima o pseudonimizzata: (i) è ciò appropriato in considerazione della finalità dell'estesa conservazione? I dati conservati in forma pseudonimizzata possono essere conservati in forma completamente anonima ed essere ancora sufficienti per la finalità specifica? Quanto è vera l'affermazione che i dati sono "resi anonimi"? (Si noti che la completa anonimizzazione è sempre più difficile da ottenere, specialmente in grandi serie di dati e soprattutto se tali serie di dati possono essere abbinate o collegate ad altre).

- Quali sono **le terze parti** a cui tali dati sono stati **comunicati**? E **per quali finalità**? I dati comunicati sono **adeguati, pertinenti e necessari** per tali finalità, **accurati e aggiornati** e, in caso affermativo, in che modo viene garantito che rimangano tali?

NB: Le risposte a quanto sopra possono in parte rimandare alle risposte alle domande precedenti.

- Su quale **base giuridica** si fonda il trattamento dei dati?
NB:

Per i dati non sensibili, la base giuridica deve essere una di quelle specificate dall'articolo 6 del RGPD, per i dati sensibili, una tra quelle previste dall'articolo 9 del RGPD.

Si noti che la base del "legittimo interesse" (articolo 6, paragrafo 1, lett. f)) non si applica al trattamento di qualsiasi dato (compresi i dati non sensibili) da parte delle autorità pubbliche nell'esecuzione dei loro compiti (articolo 6, paragrafo 1, ultima frase) e non può essere invocato da alcun titolare, nel settore pubblico o privato, per trattare dati sensibili (vedi articolo 9).

Inoltre, se il trattamento si basa sull'articolo 6 paragrafo 1, lett. (c) o (e) ("il trattamento [che] è necessario per l'adempimento di un obbligo legale a cui è soggetto il titolare del trattamento", "il trattamento [che] è necessario per l'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di pubblici poteri affidati al titolare del trattamento"), deve fondarsi sul diritto dell'Unione europea o dello Stato membro dell'UE (articolo 6, paragrafo 3). Se una delle due è la base giuridica indicata, il RPD deve verificare se la legge in questione soddisfa i requisiti di cui all'articolo 6, paragrafo 3, del RGPD.

La base giuridica richiesta è appropriata per l'elaborazione? Sono soddisfatte le condizioni pertinenti per l'applicazione della base giuridica (ad es., per quanto riguarda il consenso, come ulteriormente indicato di seguito)?

Si noti che la base giuridica per il trattamento per la finalità primaria può essere diversa da quella su cui si basa qualsiasi trattamento (incluso l'uso o la comunicazione) per qualsiasi finalità secondaria o nuova, non correlata - e la validità della presunta base giuridica deve essere valutata separatamente per ciascuna di esse.

- Se i dati vengono trattati sulla base del **consenso** degli interessati:

- **come e quando** viene ottenuto il consenso (ad es., in formato cartaceo o elettronico, da una domanda diretta o chiedendo a un individuo di spuntare una casella) [324]?

[324] Si noti che una semplice dichiarazione su un sito che dica: "*continuando ad utilizzare questo sito, acconsenti alla raccolta e uso dei tuoi dati personali*" non è più sufficiente a costituire un valido

- quale **prova** è mantenuta dell'avvenuta prestazione del consenso (ad es., copie cartacee, log)?
- come e per quanto tempo viene **conservata** questa prova?
- se nel contesto di un contratto, la tua organizzazione richiede più dati di quelli necessari per il contratto, l'interessato è informato del fatto che **non ha bisogno di fornire i dati aggiuntivi**?
- Gli interessati **sono informati** di tutte le questioni di cui dovrebbero essere messi a parte (cfr. Artt. 13 e 14 del RGPD, come riportato nel modulo dettagliato di trattamento dei dati personali, al punto II.4), e in caso affermativo, quando e come?
- Sono fornite tutte le informazioni pertinenti? Tale informativa è fornita nel miglior formato? Nel momento migliore? Le informazioni obbligatorie sono chiaramente distinte da quelle opzionali?
- Ci sono dati che sono **trasferiti a un paese terzo** [paese non UE / AEE] (o un settore in un paese terzo) o a **un'organizzazione internazionale** che è stata considerata in grado di garantire un livello "adeguato" di protezione ai sensi dell'art. 45 RGPD?
- La decisione sull'adeguatezza copre effettivamente il trattamento? È ancora valida (tenendo conto ad es. della pronuncia della Corte di Giustizia che ha ritenuto la decisione sull'adeguatezza del Safe Harbor non valida)?
- Ci sono dati che sono **trasferiti a un paese terzo** [paese non UE / AEE] (o un settore in un paese terzo) o a **un'organizzazione internazionale** che è stata considerata non in grado di garantire un livello "adeguato" di protezione ai sensi dell'art. 45 RGPD? In tal caso, quale salvaguardia o deroga è alla base del trasferimento?
- **NB**: Ai sensi del RGPD, i trasferimenti verso paesi che non sono stati ritenuti in grado di fornire una protezione "adeguata" possono aver luogo solo se sono state predisposte "**opportune salvaguardie**", come elencato nell'articolo 46 del RGPD, o se si applica una **deroga**, come indicato nell'articolo 49 RGPD (vedi sezione II.5 nel modulo dettagliato di trattamento dei dati personali, domanda 16).

  La/le salvaguardia/e o la/e deroga/he menzionate sono corrette? Soddisfa/soddisfano tutti i requisiti elencati nel relativo articolo (articolo 46 o 49)?
- Esistono regole in relazione alla notifica al titolare o al responsabile di sentenze di autorità giudiziarie o amministrative di un paese terzo, che impongano al titolare o al responsabile di trasferire o comunicare i dati personali?

NB: Ai sensi dell'articolo 48 del RGPD, le sentenze e le decisioni di paese terzi "possono essere riconosciute o assumere qualsivoglia carattere esecutivo soltanto se basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro, fatti salvi gli altri presupposti di trasferimento a norma del presente capo". Questa è una questione difficile da valutare per i referenti e molti titolari e responsabili del trattamento, e dovrebbero essere previsti orientamenti su come essi dovrebbero agire se obbligati a confrontarsi con una tale sentenza o

consenso in base al RGPD. Non solo vi sono informazioni insufficienti sull'utilizzo dei dati, che rende il "consenso" invalido posto che il consenso non è "informato". Ma è altresì dubbio se continuare la navigazione su quel sito possa essere considerato "*una manifestazione di inequivocabile dell'interessato*" (cfr. definizione di consenso, Art. 4(11) RGPD).

decisione. Per lo meno, i responsabili e i referenti dovrebbero immediatamente riferire la questione fino al più alto livello di gestione del titolare e del RPD.

Se esistono orientamenti, sono adeguati (ad es., se è stata adottata prima di entrare nella piena applicazione del RGPD, potrebbe non aver menzionato il coinvolgimento del RPD in materia, in quanto potrebbe non esserci stato un RPD quando la guida è stato redatta)? Se non ci sono ancora orientamenti in merito, dovrebbero essere predisposti con la massima urgenza, consultando il RPD per il loro contenuto.

- Quali misure formali, organizzative, pratiche e tecniche sono in atto per garantire la sicurezza e la confidenzialità dei dati?

NB: Ai sensi dell'articolo 32 del RGPD, titolari e responsabili del trattamento devono attuare "misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio" che il trattamento pone ai diritti e alle libertà delle persone fisiche (compresi in particolare gli interessati). L'articolo elenca varie misure come la pseudonimizzazione e la crittografia, clausole di riservatezza, misure tecniche per garantire l'integrità, la disponibilità e la resilienza dei sistemi utilizzati e le capacità di ripristino.

Il problema sarà ulteriormente affrontato nel Compito 3 (valutazione del rischio). Tuttavia, una **panoramica iniziale** delle misure adottate (o non adottate) dovrebbe essere già ottenuta nel contesto del Compito 2, per fornire **un'indicazione preliminare** sul fatto che le misure adottate siano "appropriate" alla luce dello "stato dell'arte", i costi di attuazione e la natura, l'ambito, il contesto e le finalità del trattamento, nonché il rischio di diversa probabilità e severità per i diritti e le libertà delle persone fisiche "(come è previsto nell'articolo 23).

Molte (anche se non tutte) delle misure sono coperte da standard internazionali riconosciuti, come quelli elencati di seguito. Tuttavia, va notato che questi non sempre coprono tutti le questioni rilevanti, ad esempio tendono a concentrarsi sulla sicurezza piuttosto che sulla minimizzazione dei dati o sul principio di finalità[325].

Anche così, i RPD dovrebbero essere a conoscenza di standard come questi - e verificare se la loro autorità di protezione dei dati o il CEPD ha preso posizione sugli stessi standard (in modo positivo o negativo, o con aggiunte):

- ISO / IEC 27001: 2013 Codice di condotta per il controllo delle informazioni

- ISO / IEC 29100 - Tecnologia dell'informazione - Tecniche di sicurezza – Quadro di riferimento Privacy

- ISO / IEC 27018 - Codice di buone prassi per la protezione delle informazioni personali nei cloud pubblici che trattano informazioni personali

- ISO / IEC 29134 - Linee guida per la valutazione dell'impatto sulla privacy (PIA)

- ISO / IEC 29151 - Codice di condotta per la protezione delle informazioni personali

[325] Alcuni anni fa le autorità di protezione dei dati notarono che un documento ISO sulla sicurezza che trattava anche il tema dei codici PIN non specificava i numeri e la natura dei caratteri che avrebbero dovuto essere utilizzati, Da quel momento le autorità hanno un orientamento volto ad interagire il più possibile con I gruppi ISO le cui attività si relazionano con le tematiche di protezione dati.

- JIS 15001: 2006 - Requisiti del sistema di gestione della protezione delle informazioni personali

- BS 10012: 2017 - Specifiche per un sistema di gestione delle informazioni personali

Ulteriori standard sono in preparazione:

- ISO 20889 - Tecniche di de-identificazione dei dati che migliorano la privacy

- ISO 29184 - Informativa sulla privacy online e consenso

- ISO 27552 Miglioramento ISO / IEC 27001 per la gestione della privacy - Requisiti - Nuovo titolo: Estensione a ISO / IEC 27001 e ISO / IEC 27002 per la gestione delle informazioni sulla privacy - Requisiti e linee guida

- Prassi di riferimento UNI - Linee guida sulla gestione dei dati personali negli ambienti ICT secondo il RGPD

Se nell'elaborazione viene utilizzato un "cloud", occorre considerare se sono state trattate le questioni elencate nelle linee guida "Trusted Cloud – Data Protection Profile for Cloud Services (TCDP)" adottate nell'ambito del progetto pilota tedesco "Data protection Certification for Cloud Services" (anche se fino ad oggi si riferiscono ancora alla legge federale tedesca sulla protezione dei dati pre-RGPD, piuttosto che al RGPD) [326].

In questa fase, il RPD deve verificare se il titolare del trattamento e/o i referenti sono a conoscenza degli standard di cui sopra, se mirano ad applicarli e, in tal caso, se esistono certificazioni in tal senso. La questione se siano effettivamente pienamente rispettati, o se dovrebbero esserlo, sarà affrontata in modo più completo nel Compito 3 (valutazione dei rischi).

Questa revisione è la prima componente della funzione del RPD "Controllo continuo della conformità" (rilevata anche nella relativa sezione dopo il compito 4).

In ogni caso, se è opinione del RPD che un trattamento dei dati personali non soddisfi i requisiti del RGPD, il RPD deve **informare** la persona o le persone internamente responsabili delle carenze e proporre azioni correttive (fino a interrompere completamente il trattamento se necessario). Nel caso in cui questo suggerimento non venga accolto, il RPD dovrebbe sottoporre il problema al top management (vedi sotto, "Attività di consulenza").

Si noti che questa revisione generale delle operazioni di trattamento è una questione separata dal caso di una violazione dei dati personali verificatasi, come discusso in relazione al Compito 6 ("Gestione delle violazioni dei dati personali"): come lì spiegato, tali violazioni devono essere immediatamente segnalate ai più alti livelli dell'organizzazione.

Il RPD dovrebbe mantenere piena **prova** di tutte le attività di riesame e valutazione e di tale segnalazione.

---

326 Cfr: https://tcdp.de/data/pdf/14_TCDP_v1.0_EN.pdf (si vedano in particolare gli elenchi di standard alle pagg. 14-16). La versione disponibile al momento della scrittura di questo manuale (V.1.0) è datata settembre 2016, ma gli autori auspicano che – dopo che gli standard di auditing e le procedure di certificazione saranno stati creati – "le certificazioni TCDP saranno convertite in certificazioni per i servizi cloud ai sensi del RGPD" (p. 7). Vedi anche la discussione sui fattori di rischio, ecc. identificati dal GEPD in relazione ai servizi cloud, discussi nel Compito 3, qui sotto.

- o – O – o -

COMPITO 3: Valutazione dei rischi posti dalle attività di trattamento di dati personali

Come rilevato al paragrafo 2.2.1, il RGPD impone ai *titolari* un obbligo generale di "[tenere] conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento nonché **dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche**" posti da ciascun trattamento di dati personali, e di "mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento" (Art. 24, paragrafo 2; si veda anche l'Art. 25, paragrafo 1).

Anche il RPD

> Nell'eseguire i propri compiti […] considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
>
> (Art. 39, paragrafo 2)

Il rispetto di tali obblighi impone l'accertamento dei rischi in questione. Tale accertamento dovrebbe essere svolto in rapporto alla definizione dell'inventario delle attività di trattamento e alla creazione di un registro di tali attività di trattamento (Compito 1) nonché, in modo particolare, all'analisi delle attività stesse (Compito 2).

Il RGPD non impone in modo esplicito che il RPD sia coinvolto in ogni esercizio di valutazione dei rischi, mentre tale coinvolgimento è previsto senza alcun dubbio in rapporto alle più approfondite valutazioni di impatto sulla protezione dei dati di cui all'Art. 35, paragrafo 2 – si veda il Compito 4, *infra*. Tuttavia, di fatto è fortemente consigliabile, quantomeno, coinvolgere il RPD anche nelle attività connesse più in generale alla valutazione dei rischi di cui sopra. In pratica, l'esito di tale valutazione dipenderà spesso dal parere del RPD.

Occorre osservare che i rischi oggetto di valutazione non si limitano ai rischi per la sicurezza intesa in senso stretto – cioè alla probabilità e all'impatto di una violazione dei dati[327] - bensì ai **rischi per i diritti e le libertà degli interessati (e di altre persone fisiche)** posti dal trattamento. Si tratta, dunque, non soltanto dei rischi per i diritti alla riservatezza e alla vita privata e per gli specifici diritti riconosciuti agli interessati, ma anche, a seconda dei casi, dei rischi per i diritti alla libertà di espressione, alla libertà di circolazione, alla non-discriminazione, alla libertà dagli autoritarismi, al diritto di vivere in una società democratica senza indebite attività di sorveglianza svolte dal proprio o da un altro Paese, e per il diritto a un rimedio giurisdizionale effettivo. Il concetto ha una valenza molto ampia.[328]

La valutazione complessiva dei rischi dovrebbe tenere conto anche delle risultanze dell'analisi condotta nel quadro del Compito 2. Per esempio, se si è rilevato che uno specifico trattamento, per quanto lecito nel senso di fondato su un'idonea base giuridica e finalizzato

[327] Per "violazione dei dati personali" si intende, ai sensi del RGPD, "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

[328] Si veda l'analisi relativa alla nozione di "rischio" e di "rischio elevato" rispettivamente nel Compito 1 (voce "Esenzioni") e nel Compito 4.

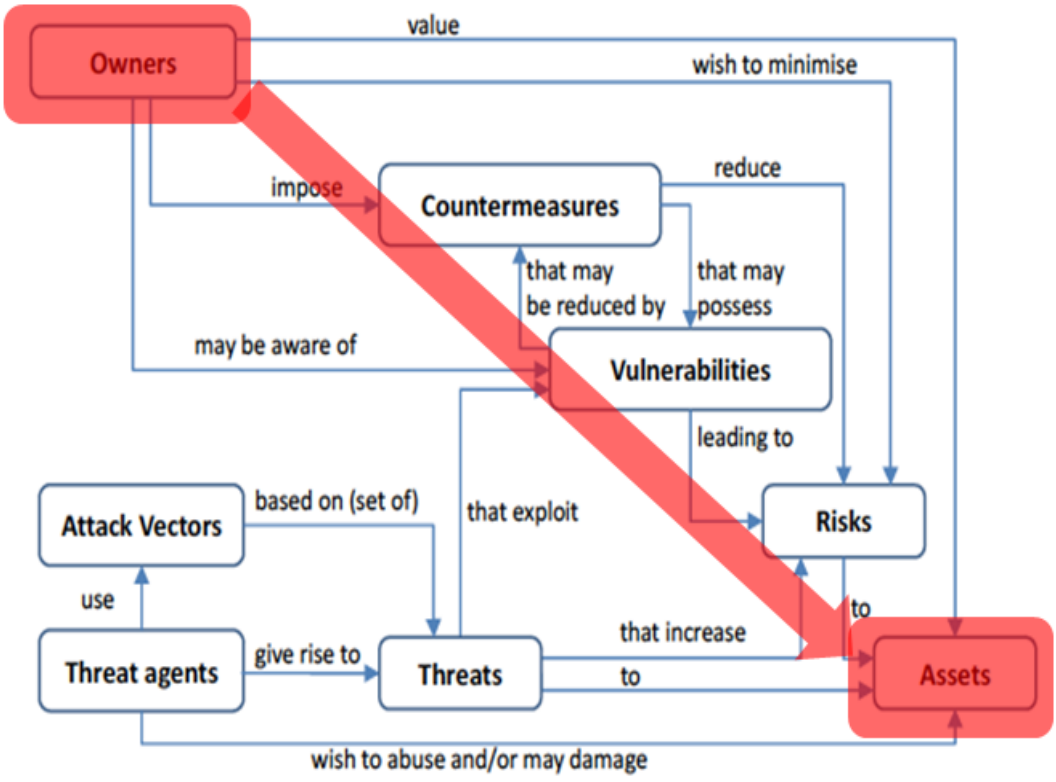
a un interesse legittimo, comporta la raccolta e la conservazione di dati non pertinenti ed eccedenti per la specifica finalità, quindi in violazione del principio di "minimizzazione dei dati", si può affermare che ciò ponga di per sé un "rischio" – ossia, il rischio di un utilizzo improprio dei dati non pertinenti ed eccedenti. In tal caso, la misura adeguata per evitare il manifestarsi di questo rischio sarebbe l'astenersi dalla raccolta dei dati non pertinenti ed eccedenti, con la cancellazione dei dati di queste tipologie già detenuti. Un altro esempio potrebbe essere l'impiego di dati ancora caratterizzabili come identificativi in un trattamento statistico che possa essere svolto attraverso dati pseudonimizzati o anonimizzati; in tal caso, la misura adeguata sarebbe quella di assicurarsi che i dati utilizzati siano pseudonimizzati correttamente o, meglio ancora, anonimizzati.

Tutto questo sottolinea la necessità per un RPD di analizzare attentemente **tutti gli aspetti di ogni singolo trattamento o funzionalità di protezione dati** – sia nell'ambito dell'analisi complessiva di cui al Compito 2, sia nel quadro della valutazione dei rischi di cui si sta trattando in questa sede.

Come proposto dal Garante italiano, è utile seguire l'approccio delineato da ENISA (l'Agenzia Ue per la sicurezza delle reti e delle informazioni), che a sua volta si basa sulla norma ISO 27005 ("Minacce, abusi, vulnerabilità in grado di generare pregiudizi per l'ente"), e quindi partire dalla considerazione più approfondita degli **elementi** che compongono la nozione di **rischio**:

Bene (vulnerabilità, controlli), **Minaccia** (profilo dell'agente responsabile della minaccia, probabilità della minaccia) e **Impatto**

La figura seguente mostra le componenti del rischio e i rapporti reciproci:



Fonte: ENISA Threat Landscape Report 2016, Figura 4: Gli elementi del rischio e loro interrelazioni secondo la norma ISO 15408:2005, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016. V. anche il report del 2017, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017.

Come sottolineato anche dal Garante, **una corretta valutazione del rischio** prevede quattro fasi:

1. Definizione del trattamento e del relativo contesto
2. Comprensione e valutazione dell'impatto sulle persone
3. Definizione di eventuali minacce e valutazione della loro probabilità (probabilità del verificarsi di minacce)
4. Valutazione del rischio (attraverso l'associazione di probabilità del verificarsi di minacce e impatto).

La prima fase (definizione del trattamento e del relativo contesto) è già stata descritta nell'ambito dei Compiti 1 e 2.

La seconda fase prevede la **definizione dei livelli di impatto**, secondo una scala che appare corretto impostare su quattro diversi livelli:

Livello di impatto	Descrizione
Basso	Piccoli inconvenienti superabili senza particolari problemi (tempo necessario per re-inserire informazioni, irritazione, ecc.)
Medio	Inconvenienti significativi, superabili con alcune difficoltà (costi aggiuntivi, mancato accesso a servizi aziendali, timori, difficoltà di comprensione, stress, piccoli disturbi fisici, ecc.)
Alto	Conseguenze significative che si dovrebbero poter superare ma con gravi difficoltà (sottrazione di liquidità, inserimento in elenchi negativi da parte di istituti finanziari, danni a beni materiali, perdita dell'impiego, ordinanze o ingiunzioni giudiziarie, compromissione dello stato di salute, ecc.)
Molto alto	Conseguenze significative o irreversibili, non superabili (perdita capacità lavorativa, disturbi psicologici o fisici cronici, decesso, ecc.)

Il Garante evidenzia **quattro aree principali di valutazione** in termini di **sicurezza dei dati**, ossia:

A. Risorse di rete e tecnologiche (hardware e software)
B. Processi/procedure connessi al trattamento
C. Soggetti e persone coinvolti nel trattamento
D. Settore di attività e scala del trattamento

Per ciascuna area di valutazione, vengono poste cinque domande; una risposta affermativa indica la presenza di un rischio, come indicato nella tabella seguente.

Il soggetto che valuta il rischio per la sicurezza può calcolare, sulla base di tali risposte, la **probabilità del verificarsi di minacce**, come spiegano i due grafici relativi che seguono la tabella di cui sopra.

Il punteggio così ricavato può essere associato al punteggio relativo all'impatto per arrivare a un **punteggio complessivo di rischio**, come evidenzia l'ultimo grafico di questa serie.

LE QUATTRO AREE PRINCIPALI DI VALUTAZIONE IN TERMINI DI SICUREZZA DEI DATI:

A. Risorse di rete e tecnologiche	**B. Processi e procedure**	**C. Soggetti e persone coinvolti**	**D. Settore di attività e scala del trattamento**
1. Vi sono parti del trattamento svolte attraverso Internet?	**6.** Ruoli e procedure relative al trattamento di dati personali sono definiti in modo incerto o insufficiente?	**11.** Il trattamento di dati personali è svolto da un numero indefinito di dipendenti?	**16.** Ritenete che il Vostro settore di attività sia passibile di attacchi cibernetici (cyberattacks)?
2. E' possibile accedere a un Sistema interno di trattamento dati attraverso Internet (per esempio, riguardo a certi utenti o gruppi di utenti)?	**7.** L'utilizzo accettabile delle risorse di rete, di Sistema e fisiche all'interno dell'ente è definito in modo incerto o insufficiente?	**12.** Vi sono parti del trattamento svolte da un agente o da un soggetto terzo (responsabile del trattamento)?	**17.** L'ente ha subito attacchi cibernetici o altre tipologie di violazioni della sicurezza negli ultimi due anni?
3. Il Sistema di trattamento dati	**8.** Ai dipendenti è consentito portare	**13.** Gli obblighi dei soggetti/delle	**18.** Sono stati ricevuti notifiche e/o

personali è interconnesso a un altro Sistema o Servizio IT interno o esterno al Vostro ente?	con sé e utilizzare i propri dispositivi collegandoli al Sistema di trattamento dati personali?	persone coinvolti nel trattamento di dati personali sono fissati in modo incerto o insufficiente?	reclami relativamente alla sicurezza dei sistemi IT (utilizzati per il trattamento di dati personali) nell'ultimo anno?
4. E' facile per soggetti non autorizzati accedere all'ambiente di trattamento dati?	**9.** Ai dipendenti è consentito trasferire, memorizzare o comunque trattare dati personali al di fuori del perimetro dell'ente?	**14.** Il personale che partecipa al trattamento di dati personali non ha conoscenze in materia di sicurezza delle informazioni?	**19.** Un trattamento riguarda volumi consistenti di dati personali e/o un numero consistente di persone fisiche?
5. Il Sistema di trattamento dati personali è progettato, implementato o manutenuto senza seguire le migliori pratiche del settore?	**10.** Le attività di trattamento dati personali possono essere svolte senza che ciò comporti la creazione di file di registrazione eventi (log files)?	**15.** I soggetti/le persone che partecipano al trattamento di dati personali omettono di conservare in modo sicuro e/o distruggere i dati personali?	**20.** Esistono migliori pratiche in materia di sicurezza specifiche del settore di attività dell'ente che non siano state implementate in misura adeguata?

PROBABILITA' DEL VERIFICARSI DI MINACCE (1):

Area di valutazione	N. di risposte affermative	Livello	Punteggio
A. Risorse di rete e tecnologiche	0 – 1	Basso	**1**
	2 – 3	Medio	**2**
	4 – 5	Alto	**3**
B. Processi e procedure	0 – 1	Basso	**1**
	2 – 3	Medio	**2**
	4 – 5	Alto	**3**

C. Soggetti e persone coinvolti	0 – 1	Basso	**1**
	2 – 3	Medio	**2**
	4 – 5	Alto	**3**
D. Settore di attività e scala del trattamento	0 – 1	Basso	**1**
	2 – 3	Medio	**2**
	4 – 5	Alto	**3**

I punteggi sopra indicati sono quindi riportati nella seguente tabella di sintesi:

PROBABILITA' DEL VERIFICARSI DI MINACCE (2):

Somma dei punteggi	**LIVELLO DI PROBABILITA' del verificarsi di minacce**
4 – 5	**Basso**
6 – 8	**Medio**
9 – 12	**Alto**

Infine, i risultati così ottenuti vengono combinati con quelli relativi al "livello di impatto" di cui alla prima tabella, ricavando un'indicazione del rischio complessivo:

VALUTAZIONE DEL RISCHIO COMPLESSIVO:

	LIVELLO DI IMPATTO			
PROBABILITA' MINACCE		**Basso**	**Medio**	**Alto/Molto alto**
	Bassa			
	Media			
	Alta			

Legenda:

[ ] Rischio basso [ ] Rischio medio [ ] Rischio elevato

SI OSSERVI, TUTTAVIA, che lo schema per la valutazione del rischio di cui sopra vale principalmente per i **rischi in materia di sicurezza dei dati**.

Si tratta indubbiamente di una classe importante di rischi che devono essere valutati e gestiti correttamente, e non una tantum ma in modo continuativo, perché i rischi possono evolvere e mutare nel tempo. Si vedano le osservazioni relative a "Controllo della conformità: Ripetizione dei compiti da 1 a 3 (e 4) su base continuativa", al termine della descrizione del Compito 4.

Tuttavia, il RGPD fa riferimento, in modo più generale, ai "rischi per i diritti e le libertà delle persone fisiche" (v. Artt. 34-36). Il primo di questi articoli (34) indica chiaramente che le violazioni dei dati di per sé possono dare luogo a rischi del tipo ora descritto, e prevede norme stringenti per la gestione di casi del genere meglio illustrate nella parte dedicata al Compito 4 (DPIA), 5 (Accertamenti), 10 (Cooperazione con l'Autorità di controllo) e 12 (Informazione e sensibilizzazione).

SI osservi, a ogni modo, che "**rischi per i diritti e le libertà delle persone fisiche" non derivano unicamente dalle violazioni dei dati**. Lo stesso RGPD prevede all'Art. 35, paragrafo 3, che "rischi elevati" di tal genere possono derivare, in particolare, da

a) 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;

b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

In tutti questi casi, e proprio per il fatto che trattamenti di questo tipo comportano **rischi intrinsecamente elevati** per i diritti e le libertà delle persone, è necessario condurre una Valutazione di impatto sulla protezione dei dati (DPIA), e in determinate circostanze consultare la o le autorità di controllo competenti (v. considerazioni relative al Compito 4).

Più specificamente, processi decisionali automatizzati basati sulla profilazione possono dar luogo a **decisioni ingiuste** (perché nessuna persona è esattamente identica a un'altra, e nessun sistema sarebbe in grado di conoscere tutto di ogni persona – o almeno ciò è auspicabile), oppure a decisioni non democratiche con **effetti discriminatori ma non sindacabili**;[329] anche l'impiego di dati sensibili può comportare **discriminazioni** (volutamente o meno)[330]; il trattamento di dati apparentemente innocui come quelli sugli acquisti effettuati può rivelare situazioni sanitarie molto personali o stati di gravidanza[331]; infine, il monitoraggio

[329] Si veda lo studio di Douwe Korff e Marie Georges dal titolo "Passenger Name Records, data mining & data protection: the need for strong safeguards" [Schede nominative dei passeggeri, data mining & protezione dati: la necessità di robuste garanzie], condotto per il Comitato consultivo della Convenzione 108/81 del Consiglio d'Europa (T-PD), 2015, paragrafo I-iii, https://rm.coe.int/16806a601b .

[330] E' per tale motivo che gli strumenti europei in materia di protezione dati prevedono norme specifiche e particolarmente restrittive per il trattamento di questi dati (v. la Nota al paragrafo 1.2.3, nella Parte I).

[331] V. *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, Forbes, 16 February 2012, visionabile qui:

sistematico delle persone in luoghi pubblici può avere **effetti paralizzanti sull'esercizio di diritti fondamentali come la libertà di espressione, associazione e protesta**.[332] In effetti, tutti questi rischi possono presentarsi in forma associata con effetti di **reciproco potenziamento**, come nel caso del ricorso alle tecniche di riconoscimento del volto per il monitoraggio di luoghi pubblici da parte delle forze di polizia, allo scopo di "identificare" potenziali delinquenti e prevedere comportamenti scorretti.[333]

Si osservi che i rischi suddetti possono manifestarsi in assenza di violazioni dei dati: essi derivano dalle caratteristiche intrinsecamente pericolose dei trattamenti in quanto tali, anche ove svolti in modo conforme alle rispettive disposizioni e senza che si verifichi alcuna violazione dei dati ai sensi del RGPD. ***Di tutto ciò non si tiene conto nello schema per la valutazione del rischio (peraltro utilissimo) sopra presentato.***

Lo stesso dicasi per quanto riguarda minori "rischi per i diritti e le libertà delle persone fisiche" derivanti da attività di trattamento non comprese nell'elenco di quelle che intrinsecamente comportano un "rischio elevato". Si tratta, in particolare, di quei trattamenti che non risultano pienamente conformi ai requisiti del RGPD.

ESEMPI:

- Utilizzo di dati personali raccolti per una determinata finalità a scopi diversi e non "compatibili" senza disporre di un'idonea base giuridica per il trattamento secondario e/o senza informare adeguatamente gli interessati degli utiizzi secondari dei loro dati che si prevede di effettuare – con l'eventuale aggravante della comunicazione dei dati a un soggetto terzo.
- Ciò può comportare l'impossibilità per gli interessati di acconsentire (o non acconsentire, od opporsi) al trattamento secondario, con possibili conseguenze negative (per esempio in caso di richieste di finanziamento o di lavoro). Vi è anche l'elevata probabilità che dati personali ottenuti in un determinato contesto non siano sufficientemente esatti o pertinenti ai fini del loro utilizzo in un contesto completamente diverso.
- Conservazione e/o utilizzo di dati personali (tipicamente, una volta cessate le esigenze connesse alla finalità iniziale del trattamento) in forma pseudonimizzata o asseritamente anonimizzata (in genere, ai fini del loro utilizzo ulteriore in questa forma per una finalità diversa e ulteriore).

https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#2ea04af16668 .

[332] V. la citazione tratta dalla famosa sentenza della Corte costituzionale tedesca in materia di censimento, a p. 13 del Manuale.

[333] V. Douwe Korff, *First Do No Harm: The potential of harm being caused to fundamental rights and freedoms by state cybersecurity interventions*, paragrafo 2.4, *Preventive, predictive policing*, in: Ben Wagner, Matthias C. Kettemann and Kilian Vieth (Eds.), Research Handbook on Human Rights & Digital Technology: Global Politics, Law & International Relations, Centre for Internet and Human Rights, Berlin, 2018

- Considerato il rischio crescente di reidentificazione anche di dati asseritamente anonimizzati[334], la conservazione prolungata e l'utilizzo di dati pseudonimizzati o asseritamente anonimizzati devono essere considerati un rischio per i diritti e le libertà degli interessati (in taluni casi, un rischio verosimilmente "elevato" tale da richiedere una valutazione di impatto sulla protezione dei dati, v. Compito 4). Il RPD deve verificare con la massima attenzione i rischi di reidentificazione di dati del genere con riguardo a eventuali utilizzi specifici, imponendo l'applicazione di robusti fattori di mitigazione (per esempio quelli tipici della "privacy differenziale")[335] nei casi opportuni, ovvero rifiutandosi di consentire l'ulteriore trattamento dei dati.
- Utilizzo di informazioni non pertinenti, inesatte o non aggiornate, con eventuali conseguenze negative di tipo analogo.
- Mancata o insufficiente considerazione degli "interessi o diritti e libertà fondamentali dell'interessato che impongono la protezione dei dati personali, in particolare qualora l'interessato sia un minore" nel valutare la possibilità di trattare dati personali sulla base del presupposto del "legittimo interesse" (Art. 6, paragrafo 1, lettera f), RGPD).
- Tutto ciò provoca, per definizione, un pregiudizio a carico degli interessi delle persone interessate. Il ricorso al criterio del "legittimo interesse" per trattare dati personali richiede sempre un'analisi particolarmente attenta da parte del RPD in questa fase.
- **NB**: Il criterio del legittimo interesse non è invocabile dai soggetti pubblici "nell'esecuzione dei loro compiti" (Art. 6, paragrafo 1, ultimo periodo); tuttavia, ciò non significa che la problematica in oggetto non si presenti mai in un contesto pubblico, per esempio in rapporto ad attività non previste specificamente in atti normativi quali l'invio di messaggi di posta elettronica a cittadini con riguardo a eventi culturali attraverso il ricorso ai registri dell'anagrafe, oppure in rapporto ad attività condotte da soggetti privati che svolgano compiti "nel pubblico interesse".
- Mancata prestazione agli interessati di tutte le dettagliate informazioni previste dagli Artt. 13 e 14 del RGPD
- La conseguenza in questo caso può consistere nell'impossibilità per l'interessato di esercitare appieno i diritti previsti dal RGPD (che rappresentano esattamente quegli "interessi o diritti e libertà fondamentali dell'interessato" meritevoli di protezione).
- Trasferimento di dati personali verso un Paese terzo che non sia stato giudicato "adeguato" in termini di protezione dei dati personali, in assenza di adeguate garanzie o del ricorso a norme vincolanti d'impresa (BCR) approvate, oppure senza fare

[334] Una chiara e sintetica illustrazione delle tematiche connesse a deidentificazione e reidentificazione è quella contenuta nel contributo della Foundation for Information Policy Research al Governo UK in occasione della consultazione denominata "Making Open Data Real", ottobre 2011, disponibile qui: www.fipr.org/111027/opendata.pdf. In tale contributo si rinvia allo studio fondamentale sul tema di Paul Ohm, "Broken Promises of privacy: responding to the surprising failure of anonymization", 57 UCLA Law Review (2010) 1701, disponibile qui: http://papers.ssrn.com/sol3/paperscfm?abstract_id=1450006.

[335] Le tecniche di privacy differenziale sono un importante strumento per impedire la reidentificazione di interessati a partire da insiemi di dati; tuttavia, esse sono efficaci soltanto se applicate in un ambiente controllato, ove è possibile un numero ristretto di interrogazioni verso lo specifico insieme di dati: si veda https://privacytools.seas.harvard.edu/differential-privacy
https://people.eecs.berkeley.edu/~stephentu/writeups/6885-lec20-b.pdf
Tali metodiche non rappresentano un ausilio qualora i dati personali siano rilasciati nel dominio pubblico in forma asseritamente anonimizzata, ovvero qualora grandi insiemi di dati siano incrociati con altri dati senza un pieno controllo.

affidamento su una delle deroghe specifiche al divieto di trasferimento dati (v. Artt. 46-48 RGPD). Ricade in questa categoria il ricorso a un servizio "cloud" in cui il o i server di appoggio siano situati in Paesi terzi.

- Come evidenziato dal GEPD nel suo dettagliato parere sull'utilizzo di servizi cloud da parte delle istituzioni dell'Ue (che dovrebbe essere studiato anche dai soggetti pubblici nazionali, visto che buona parte delle indicazioni sono valide anche nel contesto nazionale), il cloud computing pone rischi specifici che devono essere valutati con la massima attenzione dai titolari (con l'ausilio dei RPD).[336] L'indicazione che ne emerge è che si possa ben ritenere che il cloud computing comporta rischi intrinsecamente elevati e necessiti, pertanto, di una valutazione di impatto. V. al riguardo le considerazioni riferite al successivo Compito.
- Affidamento in outsourcing del trattamento di dati personali da parte di soggetti pubblici, in particolare se i dati sono sensibili a norma del RGPD ("categorie particolari di dati", Art. 9) o comunque sensibili in termini più generali (dati finanziari, dati anagrafici).
- Il GEPD rileva che il ricorso al cloud computing aumenta i rischi connessi all'outsourcing dei trattamenti.[337]

Qualora, una volta condotta la valutazione, il RPD ritenga che un trattamento di dati personali comporta rischi per gli interessi in gioco, il RPD deve **informare** di tali rischi i soggetti preposti al trattamento e proporre **misure di mitigazione o opzioni alternative**. Spesso è possibile conseguire uno scopo legittimo utilizzando strumenti diversi e meno invasivi, oppure ricorrendo a un minore volume di dati (e a dati meno sensibili); in tutti questi casi, il RPD dovrebbe formulare con decisione la propria proposta. Se tale indicazione non viene seguita, il RPD dovrebbe **riferire** la questione ai livelli più alti dell'organizzazione (v. *infra* alla voce "Compiti consultivi").

Anche in questo caso, il RPD deve **documentare** dettagliatamente tutte le valutazioni del rischio e le indicazioni formulate.

Se la proposta del RPD viene accolta, la documentazione suddetta servirà a "**dimostrare** che il trattamento è effettuato conformemente al presente Regolamento" – ossia, che i rischi in questione sono stati effettivamente valutati e che le misure adottate alla luce di tale valutazione erano adeguate al rischio rilevato (v. Art. 24, paragrafo 1, e le considerazioni sugli "obblighi di dimostrare la conformità" rispetto al RGPD al paragrafo 2.2, *supra*).

Si osservi che qualora la valutazione del rischio complessivo indichi che un trattamento cui si intende procedere può comportare un "rischio elevato" per i diritti e le libertà delle persone fisiche, il RPD deve informare il titolare della necessità di condurre una valutazione di impatto sulla protezione dei dati (DPIA) nei termini esaminati al punto successivo (Compito 4).

---

[336] Garante europeo per la protezione dei dati (GEPD), Guidelines on the use of cloud computing services by the European institution and bodies, marzo 2018, disponibile qui:
https://edps.europa.eu/sites/edp/files/publication/18-03-16_cloud_computing_guidelines_en.pdf
V. in particolare l'Allegato (Annex) *4: Data protection-specific risks of cloud computing*

[337] Le Linee-guida del GEPD sopra menzionate (v. nota precedente) "si concentrano sul ricorso a servizi cloud forniti da soggetti commerciali [ma] in tal senso esaminano anche le problematiche sollevate dall'outsourcing di servizi IT che trattino dati personali" (p. 5).

SI osservi, inoltre, che anche ove non sia richiesta una DPIA, il RPD dovrà monitorare tutti i trattamenti svolti dal titolare su base continuativa: si vedano le considerazioni svolte dopo il punto 4, alla voce "Monitoraggio della conformità: ripetizione dei compiti da 1 a 3 (e 4) su base continuativa".

Si tenga presente che spesso il legislatore nazionale ha già tentato una prima gestione dei rischi particolari che si ritengono associati a determinate attività di trattamento, attraverso le norme nazionali; tutto ciò continua a trovare spazio, in larga parte, nella "flessibilità" che caratterizza alcune disposizioni del RGPD.[338]

Esempi:

In Croazia, è vietato il trattamento di **dati genetici** per il calcolo del rischio dell'insorgenza di patologie o di altri eventi sanitari in rapporto alla stipula o all'esecuzione di contratti assicurativi sulla vita e di contratti contenenti clausole sui benefici in caso di sopravvivenza; tale divieto non è superabile neppure con il consenso dell'interessato (Art. 20 della Legge di attuazione del RGPD).

Come in altri Paesi, il ricorso a **dati biometrici** e l'impiego di **sistemi di videosorveglianza** sono soggetti a condizioni specifiche quali il requisito di un consenso particolarmente inequivocabile ed esplicito, e ad alcuni vincoli relativi, per esempio, a limitazioni del periodo di conservazione dei dati.

Previsioni di legge quali quelle sopra indicate devono essere tenute presenti nella valutazione del rischio: nessun titolare o RPD potrebbe mai giungere alla conclusione che un determinato rischio sia accettabile pur in violazione delle specifiche disposizioni o limitazioni previste per legge.

***

[338] V. la Parte II, paragrafo 2.2.

COMPITO 4 GESTIONE DEI TRATTAMENTI CHE POSSONO COMPORTARE UN "RISCHIO ELEVATO": COME SI CONDUCE UNA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

Quanto detto nella sezione precedente rispetto alla valutazione complessiva del rischio (Compito 3) vale *a fortiori* per i trattamenti che, sulla base di tale valutazione complessiva dei rischi, si ritiene possano comportare un "**rischio elevato** per i diritti e le libertà delle persone fisiche" (Art. 35, paragrafo 1). Il RGPD chiarisce che ciò può verificarsi in particolare con riguardo all'utilizzazione di "nuove tecnologie".

Se la valutazione preliminare del rischio condotta nei termini indicati al Compito 3 mostra effettivamente che un determinato trattamento può comportare un "rischio elevato", il titolare è tenuto a condurre una **valutazione di impatto sulla protezione dei dati** (DPIA) prima di procedere al trattamento.

Il RGPD prevede che una DPIA debba essere condotta in ogni caso in presenza di decisioni automatizzate basate su trattamenti automatizzati/profilazione, trattamenti su larga scala di dati sensibili, o monitoraggio su larga scala di aree accessibili al pubblico (Art. 35, paragrafo 3). Le Autorità nazionali di protezione dati devono, inoltre, adottare elenchi di trattamenti soggetti al requisito della DPIA sul proprio territorio, e possono adottare elenchi di trattamenti che non sono soggetti a tale requisito; tuttavia, gli elenchi in questione devono essere sottoposti al Comitato europeo della protezione dei dati e possono essere sindacati da altre Autorità attraverso il cosiddetto "meccanismo di coerenza" (Art. 35, paragrafi 4-6). Il RGPD permette al Comitato stesso di redigere un proprio elenco negativo e positivo, sulla base di quelli presentati dalle Autorità nazionali di protezione dati (che sono tenute a sottoporre i rispettivi elenchi ai sensi dell'Art. 64, paragrafo 1, lettera a) del RGPD).

Quello che è avvenuto è schematizzabile come segue. Il WP29 ha pubblicato orientamenti e linee-guida dettagliate sulla conduzione di una DPIA, sia attraverso le Linee-guida sui RPD del dicembre 2016, poi riviste ad aprile 2017 (WP243rev1)[339] sia nelle successive, e più specifiche, Linee-guida sulla valutazione di impatto (DPIA), adottate il 4 aprile 2017 e successivamente emendate e adottate nuovamente il 4 ottobre 2017 (quindi sempre prima della piena applicazione del RGPD).[340] Entrambi i documenti sono stati recepiti dal Comitato europeo per la protezione dei dati il giorno in cui il RGPD è divenuto di piena applicazione, cioè il 25 maggio 2018. Anche il GEPD ha fornito utili orientamenti attraverso un documento dal titolo "Accountability on the ground"[341], in cui si trova anche un elenco provvisorio di trattamenti che, a giudizio del GEPD, necessitano o meno di una DPIA.

Le Linee-guida sulla DPIA, riviste e adottate dal WP29 e quindi fatte proprie dal Comitato, individuano **nove criteri** di cui tener conto per stabilire se un trattamento può comportare un "rischio elevato". Vi si afferma quanto segue:

---

[339] V. nota 239, *supra*

[340] Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 (WP248rev.1, nel prosieguo "Linee-guida sulla DPIA" del WP29) disponibili qui: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

[341] EDPS, Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments , Parte 4, *When to carry out a DPIA?*, pp. 9 – 11.

Un titolare può ritenere, **nella maggioranza dei casi**, che quando un trattamento soddisfa **due** dei **criteri** sopra indicati sia necessario condurre una DPIA. In linea di principio, il Gruppo di lavoro ritiene che quanto maggiore è il numero dei criteri soddisfatti da un determinato trattamento, tanto maggiore è la probabilità che esso presenti un rischio elevato per i diritti e le libertà degli interessati e, quindi, che si renda necessaria una DPIA indipendentemente dalle misure che il titolare prevede di adottare.

Questa tematica è oggetto di un paragrafo più avanti dal titolo "Come valutare se un trattamento può comportare 'rischi elevati' ", dove sono forniti alcuni esempi tratti dalle Linee-guida del WP29 e dal documento del GEPD.

Occorre segnalare in proposito che la maggior parte delle Autorità nazionali di protezione dati (22 su 28) [compresa l'Italia] hanno adottato un elenco provvisorio sottoponendolo al parere del Comitato. Il Comitato ha analizzato tali elenchi alla luce delle Linee-guida del WP29 precedentemente recepite, e il 25 settembre 2018 ha pubblicato 22 pareri, uno per ciascun progetto di elenco.[342] Il rilievo fondamentale mosso dal Comitato in tutti i pareri suddetti consisteva nella raccomandazione alle Autorità di non comprendere nell'elenco dei trattamenti obbligatoriamente soggetti a DPIA quei trattamenti per i quali risultasse soddisfatto *uno solo* dei criteri sopra indicati ai fini della decisione sulla possibile sussistenza di un "rischio elevato" di cui alle Linee-guida. Per esempio, nel parere relativo al progetto di elenco sottopostogli dal Regno Unito[343], il Comitato scrive quanto segue:

L'elenco presentato dall'Autorità di controllo del Regno Unito ai fini del parere del Comitato afferma che il trattamento di dati biometrici comporta l'obbligo di condurre una DPIA. Il Comitato ritiene che il trattamento di dati biometrici di per sé non sia tale da poter comportare necessariamente un rischio elevato. Tuttavia, il trattamento di dati biometrici finalizzato all'identificazione univoca di una persona fisica associato ad almeno un ulteriore criterio necessita di una DPIA. Pertanto, il Comitato chiede all'Autorità di controllo del Regno Unito di emendare l'elenco in conseguenza, aggiungendo nella voce relativa al trattamento di dati biometrici finalizzato all'identificazione univoca di una persona fisica che l'obbligo di condurre una DPIA sussiste solo se tale trattamento è associato ad almeno un altro criterio, fatto salvo quanto previsto dall'Art. 35, paragrafo 3, RGPD.

Naturalmente, il titolare può condurre una DPIA anche se uno solo dei criteri in questione risulta soddisfatto – su base esclusivamente discrezionale.

Il requisito della DPIA non trova applicazione qualora lo specifico trattamento sia disciplinato da una norma e nel contesto dell'adozione di tale norma sia stata condotta una DPIA di livello generale (Art. 35, paragrafo 10). Inoltre, "Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi" (Art. 35, paragrafo 1, ultimo periodo). Come sintetizzato dal WP29:

Quando non è necessario condurre una DPIA? Quando il trattamento non "*può comportare un rischio elevato*" o esiste una DPIA simile, o il trattamento è già stato autorizzato prima del maggio 2018, o ha una base legale [SIC], o è compreso nella lista dei trattamenti che non richiedono una DPIA.

[342] Disponibili attraverso i collegamenti ipertestuali pubblicati qui: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en .

[343] Vedi il Parere 22/2018 del Comitato, relativo al progetto di elenco DPIA del Regno Unito, adottato il 25 settembre 2018 e disponibile qui: https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art._64_uk_sas_dpia_list_en.pdf .

Alcune autorità nazionali, come quella francese, spagnola e britannica, hanno pubblicato orientamenti dettagliati sulla DPIA, anche di tipo metodologico; lo stesso dicasi per il *Datenschutzzentrum* tedesco (i cui orientamenti sono stati fatti propri dalle Autorità tedesche). L'autorità francese di protezione dati (la CNIL) ha, inoltre, messo a punto un software open-source per la DPIA, in collaborazione con altre autorità, il cui obiettivo è "supportare i titolari nell'assicurare e dimostrare l'osservanza del RGPD". Sul sito web[344] si spiega quanto segue:

Chi può utilizzare il software PIA?

Questo tool è destinato principalmente ai titolari che hanno scarsa familiarità con la PIA. E' infatti scaricabile una versione stand-alone che potrà essere lanciata con grande facilità sul vostro computer.

Inoltre, si può utilizzare il tool sui server di un ente per integrarlo con altri tool o sistemi già disponibili a livello interno.

Di cosa si tratta?

Il tool PIA è stato progettato secondo tre criteri fondamentali:

- **Un'interfaccia didattica per la conduzione della PIA:** il tool utilizza un'interfaccia a misura di utente che consente di gestire la PIA facilmente. Presenta passo dopo passo la metodologia da seguire per la PIA. Vari tool di visualizzazione consentono di comprendere rapidamente i contesti di rischio.
- **Una base di conoscenze tecniche e giuridiche**: Il tool presenta i criteri giuridici atti a garantire la liceità del trattamento e i diritti degli interessati. Dispone anche di una base di conoscenze contestuale, visionabile lungo le varie fasi della PIA, che adatta i contenuti volta per volta visualizzati allo specifico aspetto del trattamento oggetto di analisi. I dati sono estratti dal RGPD, dalle linee-guida sulla PIA e dalla Guida alla sicurezza pubblicata dalla CNIL.
- **Un tool modulare**: allo scopo di aiutarvi a garantire l'osservanza, potete personalizzare i contenuti del tool secondo le specifiche esigenze o il settore di attività, per esempio creando un modello di PIA che potrete riprodurre e utilizzare per una serie di trattamenti analoghi. Il tool è pubblicato con una licenza di utilizzazione illimitata, ed è possibile modificare il codice sorgente per aggiungere componenti o integrarlo in altri tool utilizzati nel vostro ente.

Non è questa la sede per esaminare tutte le dettagliate indicazioni sulla DPIA fornite nel documento del WP29 (e poi del Comitato), o attraverso gli orientamenti pubblicati dalle autorità nazionali. **Il lettore è invitato a studiare con attenzione le linee-guida del WP29/del**

[344] Si veda https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment
La CNIL utilizza l'acronimo "PIA", presumibilmente perché la DPIA deriva dal "Privacy Impact Assessment" (PIA, valutazione di impatto privacy). Si osservi che il tool qui descritto è stato recentemente aggiornato. Per informazioni (solo in francese), si può consultare questa pagina:
https://www.cnil.fr/fr/loutil-pia-mis-jour-pour-accompagner-lentree-en-application-du-rgpd
Nella pagina sopra indicata, la CNIL afferma che il software è disponibile in 14 versioni linguistiche, fra cui francese, inglese, italiano, tedesco, polacco, ungherese, spagnolo, olandese, romeno e greco, e che ha ricevuto l'approvazione (almeno in via provvisoria, nella versione beta) di varie autorità di protezione dati (Baviera, Italia, Finlandia, Ungheria, Polonia, Norvegia). Si osservi, in ogni caso, che il software si concentra principalmente sulla sicurezza tecnica, e sarà utile soprattutto alle PMI più che a soggetti complessi e di maggiori dimensioni.

Comitato, nonché le indicazioni fornite a livello nazionale ove pertinenti, e ad applicarle in ogni ambito di attività anche di natura consulenziale.

Soprattutto i RPD dovrebbero, poi, tenere presente l'elenco nazionale dei trattamenti obbligatoriamente soggetti a DPIA pubblicato dalla rispettiva autorità di controllo; tale elenco contiene, infatti, esempi di situazioni in cui l'applicazione degli orientamenti sopra ricordati ha portato a imporre la conduzione di una DPIA da parte di soggetti pubblici e privati. I RPD sono chiamati a vigilare sulla conduzione di una DPIA a opera dei rispettivi titolari ogniqualvolta ciò risulti obbligatorio sulla base dei suddetti elenchi. Se nei prossimi mesi saranno pubblicate anche le cosiddette "Liste bianche" (ai sensi dell'Art. 35, paragrafo 5, del RGPD), anch'esse rappresenteranno un utile strumento perché escluderanno la necessità per il titolare di pensare in termini di DPIA con riguardo a tutta una serie di trattamenti a rischio non elevato.

Nei paragrafi seguenti esamineremo brevemente i principali orientamenti relativi a: **i diversi ruoli e le responsabilità di titolare e RPD**; la metodologia utile a **valutare se un trattamento possa comportare un "rischio elevato"**; le varie **metodologie per la conduzione di una DPIA**; come gestire la **documentazione della DPIA,** in particolare qualora si concluda che alcuni rischi elevati individuati tramite la DPIA stessa non siano mitigabili a sufficienza attraverso le varie misure implementabili – nel qual caso il RGPD prescrive la **consultazione obbligatoria della competente Autorità di controllo** (Art. 36).

I diversi ruoli e le responsabilità di titolare e RPD in rapporto alla DPIA

Nelle Linee-guida sul RPD, il WP29 sottolineava, ancora una volta, la diversità dei ruoli e delle responsabilità rispettivamente pertinenti al titolare e al RPD, anche con riguardo alla DPIA. Si legga quanto segue:

> In base all'articolo 35, paragrafo 1, spetta al titolare del trattamento, e non al RPD, condurre, ove necessario, una valutazione di impatto sulla protezione dei dati (DPIA, nell'acronimo inglese). Tuttavia, il RPD svolge un ruolo fondamentale e di grande utilità assistendo il titolare nello svolgimento di tale DPIA. In ossequio al principio di "protezione dei dati fin dalla fase di progettazione" (o data protection by design), l'articolo 35, paragrafo 2, prevede in modo specifico che il titolare "si consulta" con il RPD quando svolge una DPIA. A sua volta, l'articolo 39, paragrafo 1, lettera c) affida al RPD il compito di "fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35".

Il Gruppo di lavoro raccomanda che il titolare del trattamento si consulti con il RPD, fra l'altro, sulle seguenti tematiche: [345]

- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre la DPIA con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;

[345] I compiti del RPD sono elencati all'articolo 39, paragrafo 1, ove si specifica che il RPD deve svolgere "almeno" i compiti in questione. Ne deriva che niente vieta al titolare di assegnare al RPD compiti ulteriori rispetto a quelli espressamente menzionati all'articolo 39, paragrafo 1, ovvero di specificare ulteriormente i suddetti compiti.

- se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD.

Qualora il titolare del trattamento non concordi con le indicazioni fornite dal RPD, è necessario che la documentazione relativa alla DPIA riporti specificamente per iscritto le motivazioni per cui si è ritenuto di non conformarsi a tali indicazioni.[346]

Inoltre, il Gruppo di lavoro raccomanda che il titolare del trattamento definisca con chiarezza, per esempio nel contratto stipulato con il RPD, ma anche fornendo informative ai dipendenti, agli amministratori e, ove pertinente, ad altri aventi causa, i compiti specificamente affidati al RPD e i rispettivi ambiti, con particolare riguardo alla conduzione della DPIA.

Anche nelle successive Linee-guida sulla DPIA, il WP29 sottolinea che la DPIA deve essere condotta "dal titolare, insieme al RPD e ai responsabili del trattamento".

In concreto, e soprattutto negli enti di minori dimensioni, il RPD si troverà spesso, ancora una volta, a svolgere un ruolo di primo piano (se non determinante) ai fini di tale valutazione.

Come valutare se un trattamento che ci prefigge di realizzare possa comportare un "rischio elevato"

Nelle Linee-Guida sulla DPIA, il WP29/il Comitato spiega che:

> L'obbligo per i titolari del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati va inteso nel contesto dell'obbligo generale, cui gli stessi sono soggetti, di gestire adeguatamente i rischi presentati dal trattamento di dati personali.

Ossia, come già rilevato, la domanda sulla necessità o meno di condurre una DPIA deriva naturalmente dall'obbligo generale cui è soggetto il titolare – con la consulenza o, molto spesso, l'assistenza del RPD – di valutare i rischi connessi a tutti i trattamenti svolti dal titolare stesso (v. Compito 3, *supra*).

Il documento prosegue poi chiarendo la nozione di "rischio" e gli interessi meritevoli di tutela dei quali tener conto:

> Un "rischio" è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. La "gestione dei rischi", invece, può essere definita come l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi.
>
> L'articolo 35 fa riferimento al possibile rischio elevato "per i diritti e le libertà delle persone fisiche". Come indicato nella dichiarazione del gruppo di lavoro articolo 29 sulla protezione dei dati sul ruolo di un approccio basato sul rischio nei quadri giuridici in materia di protezione dei dati, il riferimento a "diritti e libertà" degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la libertà

[346] L'articolo 24, paragrafo 1, prevede che "Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario".

> di parola, la libertà di pensiero, la libertà di circolazione, il divieto di discriminazione, il diritto alla libertà di coscienza e di religione.

Il WP29 evidenzia gli esempi, contenuti all'Art. 35, paragrafo 3, del RGPD, di situazioni che comportano intrinsecamente "rischi elevati", alle quali si è già fatto cenno: qualora un titolare ricorra ad algoritmi automatizzati, basati sulla profilazione, per assumere decisioni che producono effetti giuridici o comunque effetti significativi di altra natura; qualora un titolare tratti dati sensibili o dati relativi a condanne penali "su larga scala"; o qualora un titolare "effettui il monitoraggio sistematico" di un'area accessibile al pubblico "su larga scala". Aggiunge, correttamente, che:

> Come indicato dalle parole "in particolare" nella frase introduttiva dell'articolo 35, paragrafo 3, del regolamento generale sulla protezione dei dati, questo va inteso come un elenco non esaustivo. Vi possono essere operazioni di trattamento a "rischio elevato" che non trovano collocazione in tale elenco ma che presentano tuttavia rischi altrettanto elevati.

Il WP29 elenca una serie di fattori, connessi in buona parte, ma non esclusivamente, ai tre esempi di cui all'Art. 35, che indicano come un trattamento comporti "rischi elevati" e fornisce ulteriori esempi più dettagliati. Il GEPD presenta ulteriori esempi in merito, sia con riguardo all'elenco provvisorio di trattamenti obbligatoriamente soggetti a DPIA, sia attraverso un modello utilizzabile per valutare se trattamenti che non figurano né nella lista "positiva" (trattamenti che, a giudizio del GEPD, richiedono sempre una DPIA) né nella lista "negativa" (trattamenti che, a giudizio del GEPD, non necessitano di una DPIA) debbano essere sottoposti a DPIA. Tutti questi esempi proposti dal WP29 e dal GEPD sono presentati qui di seguito, con alcune modifiche; in particolare, gli esempi del WP29 sono inseriti nei singoli box, e quelli del GEPD sono segnalati da un asterisco. Abbiamo aggiunto ulteriori esemplificazioni o particolari ovvero varianti ulteriori, di interesse per i titolari del settore pubblico; questi ultimi esempi sono indicati in corsivo.

Fattori che indicano un "rischio elevato"[347]

1. Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato" (considerando 71 e 91).

> Esempi
>
> Un ente finanziario che esamina i suoi clienti rispetto a una banca dati di riferimento in materia di crediti oppure rispetto a una banca dati in materia di lotta contro il riciclaggio e il finanziamento del terrorismo (AML/CTF) oppure contenente informazioni sulle frodi;
>
> Una banca che esamina le operazioni conformemente al diritto applicabile per individuare eventuali operazioni fraudolente.*

[347] L'ordine dei fattori è quello indicato nel documento del WP29; anche le osservazioni fondamentali relative a ciascun fattore sono tratte da quest'ultimo documento. SI osservi che vi possono essere sovrapposizioni o associazioni fra i singoli fattori come evidenziato nei paragrafi seguenti.

Profilazione applicata al personale sulla base di tutte le transazioni registrate nel sistema di gestione pratiche dell'ente, con riassegnazione automatica delle pratiche.*

Un'impresa di biotecnologie che offre test genetici direttamente ai consumatori per valutare e prevedere i rischi di malattia o per la salute;

Un'impresa che crea profili comportamentali o per la commercializzazione basati sull'utilizzo del proprio sito web o sulla navigazione sullo stesso.

2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente: trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che "hanno effetti giuridici" o che "incidono in modo analogo significativamente su dette persone fisiche" (articolo 35, paragrafo 3, lettera a)). Ad esempio, il trattamento può portare all'esclusione o alla discriminazione nei confronti delle persone.

Esempi:

Valutazione automatica del personale ("se ricadi nella decade percentile più bassa per numero di pratiche evase, riceverai una valutazione di "insoddisfacente" senza possibilità di discussione").*

Identificazione di "probabili" o "possibili" evasori fiscali attraverso l'attribuzione automatica di profili ai contribuenti.[348]

Identificazione di "probabili" o "possibili" frodi a carico del sistema di welfare sulla base di un profilo di soggetti responsabili e già noti.

Identificazione di minori "a rischio" di sviluppare obesità in età adulta o di aderire a bande criminali, oppure di minori "a rischio" di gravidanza in età adolescenziale, sulla base di profili.

Identificazione di minori e adulti "a rischio" di "radicalizzazione".

3. Monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico" (articolo 35, paragrafo 3, lettera c))15. Questo tipo di monitoraggio è un criterio in quanto i dati personali possono essere raccolti in circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà. Inoltre, può essere impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico);

[348] Questo tipo di profilazione è stata effettuata in Italia dall'Agenzia delle entrate con uno strumento denominato "Redditometro". I profili si basavano anche su previsioni di spesa da parte dei contribuenti ricavate, attraverso parametri statistici, dalla collocazione di tali contribuenti in specifiche categorie familiari o aree geografiche. Questo strumento di profilazione è stato oggetto di accertamenti da parte del Garante italiano; una delle problematiche più gravi riguardava la scarsa qualità delle informazioni e il tasso di errore conseguentemente elevato a causa delle inferenze inaffidabili compiute sulla base di tali dati. A seguito degli accertamenti condotti, il Garante ha prescritto che il calcolo del reddito effettivo del contribuente avvenisse esclusivamente sulla base di spese reali e documentate, anziché essere ricavato da ipotesi statistiche sul livello di spesa. Si veda: https://www.garanteprivacy.it/en/home/docweb/-/docweb-display/docweb/2765110 .

Esempi:

Analisi del traffico Internet violando misure di cifratura*

Videosorveglianza occulta*

Videosorveglianza intelligente (ossia, associata a software per il riconoscimento del volto) in luoghi pubblicamente accessibili*

Strumenti per la prevenzione della perdita di dati che violino misure di cifratura SSL*

Trattamento di metadati (tempo, natura, durata di una transazione bancaria) per scopi organizzativi o per ricavare stime di bilancio

4. Dati sensibili o dati aventi carattere altamente personale: questo criterio include categorie particolari di dati personali così come definite all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'articolo 10. Un esempio potrebbe essere quello di un ospedale generale che conserva le cartelle cliniche dei pazienti oppure quello di un investigatore privato che conserva i dettagli dei trasgressori. Al di là di queste disposizioni del regolamento generale sulla protezione dei dati, alcune categorie di dati possono essere considerate aumentare il possibile rischio per i diritti e le libertà delle persone fisiche. Tali dati personali sono considerati essere sensibili (nel senso in cui tale termine è comunemente compreso) perché sono legati ad attività a carattere personale o domestico (v. il terzo esempio, *infra*) oppure perché influenzano l'esercizio di un diritto fondamentale (v. il quarto esempio, *infra*) oppure perché la violazione in relazione a tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato (v. il quinto esempio, *infra*). A questo proposito, può essere rilevante il fatto che tali dati siano stati resi pubblici dall'interessato o da terzi. Il fatto che i dati personali siano di dominio pubblico può essere considerato un fattore da considerare nella valutazione qualora fosse previsto che i dati venissero utilizzati ulteriormente per determinate finalità (v. il settimo esempio, *infra*).

Esempi:

Un ospedale (o un'agenzia di welfare che conservi le cartelle sanitarie dei pazienti (o dei richiedenti sussidi o assistenza)

Un investigatore privato che conservi informazioni su condanne penali o reati (o un soggetto pubblico, per esempio un'istituzione scolastica, che conservi tali informazioni in rapporto a studenti o alunni)

Un soggetto pubblico o privato (un datore di lavoro) che acceda a documenti privati, email personali, diari o appunti tratti da lettori elettronici dotati di strumenti per la presa di appunti e di proprietà del personale (oppure utilizzati dal personale per scopi sia privati sia professionali, per esempio in contesti BYOD – Bring Your Own Device)

Un soggetto pubblico o privato (un datore di lavoro) che acceda a informazioni strettamente personali contenute in applicazioni che registrano le attività quotidiane delle persone, oppure che utilizzi informazioni tratte dai social media in contesti che

possono avere impatti significativi sugli interessati, per esempio ai fini del reclutamento occupazionale o in rapporto a colloqui di lavoro.

Esami sanitari e verifiche del casellario giudiziale precedenti l'assunzione.*

Indagini amministrative e procedimenti disciplinari.*

Qualunque utilizzo di meccanismi di identificazione biometrica del tipo 1:n.*

Fotografie utilizzate unitamente a software per il riconoscimento del volto o per ricavare altri dati sensibili (per esempio qualora ciò possa comportare effetti discriminatori in previsione dell'eventuale assunzione)*

5. Trattamento di dati su larga scala: il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91.[349] A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala: a. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; b. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; c. la durata, ovvero la persistenza, dell'attività di trattamento; d. la portata geografica dell'attività di trattamento.

Esempi:

Database nazionali o interconnessi a livello UE per la sorveglianza su determinate patologie*

Scambi di dati su larga scala fra titolari del settore pubblico (ministeri, autorità regionali e locali, ecc.) su reti telematiche.

Raccolta su larga scala di informazioni genealogiche relative a famiglie appartenenti a uno specifico gruppo religioso

Creazione di ampi database sulle abitudini di vita per scopi di marketing (ma utilizzabili anche per altri scopi)

Registrazione a opera di partiti politici delle intenzioni di voto relative a grandi numeri di elettori (o di famiglie) a livello nazionale o locale, sulla base di interviste a domicilio, con successiva analisi e utilizzazione di tali dati[350]

[349] Il considerando 91 si esprime in questi termini: "trattamenti su larga scala, 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, ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una nuova tecnologia su larga scala, (…)

[350] Si tratta di una prassi diffusa soprattutto nel Regno Unito, come riconosce lo stesso considerando 56 del RGPD, ove si afferma che "ciò può essere consentito per ragioni di pubblico interesse, purché siano definite garanzie adeguate". Quanto meno, occorre stabilire se il trattamento sia effettivamente finalizzato all'interesse pubblico, e l'obbligo di prevedere "garanzie adeguate" evidenzia l'esigenza di una seria analisi del rischio con adeguata valutazione di impatto.

6. Creazione di corrispondenze o combinazione di insiemi di dati, in particolare a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato.

> Esempi:
>
> Verifiche incrociate e non trasparenti delle registrazioni sugli accessi, degli accessi informatici, e delle dichiarazioni rese ai fini della compensazione oraria, per individuare casi di assenteismo*
>
> Un'agenzia fiscale che confronti i dati delle dichiarazioni dei redditi con gli atti di proprietà relativi a imbarcazioni di pregio, al fine di individuare potenziali evasori fiscali.

7. Dati relativi a interessati vulnerabili: il trattamento di questo tipo di dati è un criterio a motivo dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti. Gli interessati vulnerabili possono includere i **minori** (i quali possono essere considerati non essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati), i **dipendenti**, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (**infermi di mente, richiedenti asilo o anziani**, **pazienti**, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento.

> Esempi:
>
> Utilizzo di sistemi di videosorveglianza e geolocalizzazione che consentono la sorveglianza remota delle attività svolte dai dipendenti.
>
> Ogni trattamento di dati personali relativo a qualsiasi delle categorie di soggetti vulnerabili sopra ricordate, e indubbiamente ogni trattamento di dati sensibili riferiti a tali soggetti, oppure trattamenti su larga scala di dati di questo tipo relativi a soggetti vulnerabili.

8. Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative: Il regolamento generale sulla protezione dei dati chiarisce (articolo 35, paragrafo 1 e considerando 89 e 91) che l'uso di una nuova tecnologia, definita "in conformità con il grado di conoscenze tecnologiche raggiunto" (considerando 91), può comportare la necessità di realizzare una valutazione d'impatto sulla protezione dei dati. Ciò è dovuto al fatto che il ricorso a tale tecnologia può comportare nuove forme di raccolta e di utilizzo dei dati, magari costituendo un rischio elevato per i diritti e le libertà delle persone. Infatti, le conseguenze personali e sociali dell'utilizzo di una nuova tecnologia potrebbero essere sconosciute. Una valutazione d'impatto sulla protezione dei dati aiuterà il titolare del trattamento a comprendere e trattare tali rischi, e le misure di mitigazione del rischio dovrebbero consentire agli interessati e alla collettività in generale di comprendere come, quando e per quali scopi le nuove tecnologie possano essere utilizzate, in modo da difendersi dalle applicazioni in grado di pregiudicare i

diritti e le libertà delle persone favorendo derive autoritarie o forme di sorveglianza di massa, anche da parte di soggetti privati.

Nota: Per molte di queste tecnologie o prassi, le Autorità di controllo o il Comitato pubblicheranno o hanno già pubblicato orientamenti, pareri o raccomandazioni, e i RPD dovrebbero tenersi al corrente monitorando gli eventuali sviluppi. Se un RPD ritiene che non vi siano orientamenti o altri documenti di interesse, dovrebbe consultare la rispettiva Autorità di controllo. Si vedano anche i paragrafi dedicati ai Compiti 4, 8 e 10, *infra*.

Esempi:

Associazione di impronte digitali e riconoscimento del volto per migliorare il controllo sugli accessi fisici.[351]

Nuove tecnologie finalizzate a tracciare tempi e presenze dei dipendenti, comprese tecnologie che trattino dati biometrici o altre tecnologie per il tracciamento di dispositivi mobili.

Trattamento di dati generati dall'utilizzo di applicazioni appartenenti all' "Internet delle cose" (dispositivi connessi o oggetti "intelligenti"), qualora l'impiego dei dati abbia (o possa avere) impatti significativi sulla vita e la privacy delle persone.

Tecniche di apprendimento automatico.*

Interconnessione di veicoli.*

Screening di candidati all'impiego attraverso i social media.*

9. Quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto" (articolo 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.

Esempi:

Una banca che esamini i suoi clienti rispetto a una centrale rischi per il credito al fine di decidere se offrire loro un prestito o meno.

Un istituto finanziario o una centrale rischi per il credito che tenga conto della differenza di età fra i coniugi al fine di definire l'affidabilità creditizia (il che può ostacolare il libero esercizio del diritto fondamentale di contrarre matrimonio, e in Francia tale prassi è stata vietata, per esempio, dalla CNIL nell'ambito della procedura di "autorizzazione preliminare" prevista in precedenza per i trattamenti basati su profilazione)

Database negativi (di esclusione rispetto a determinate prestazioni).*

[351] Il WP29 e numerose autorità nazionali hanno pubblicato orientamenti specifici sul tema, prevedendo, fra l'altro, che i dati biologici siano memorizzati sul microprocessore presente nel device detenuto dall'interessato anziché in un database unico controllato dal titolare. Si veda il Documento di lavoro sulla biometria del WP29 (WP80 del 1 agosto 2003), successivamente emendato.

Screening creditizio.*

Trattamenti a rischio elevato per la presenza di più fattori di rischio

I fattori sopra evidenziati possono talora sovrapporsi o presentarsi in forma associata, per esempio il "monitoraggio sistematico" può associarsi e in parte sovrapporsi alle decisioni automatizzate basate su profilazione, e può comportare trattamenti "su larga scala" di dati "sensibili". Il WP29 fornisce numerosi esempi di trattamenti caratterizzati da questa combinazione multifattoriale e tali, quindi, da necessitare di una DPIA, nonché esempi di trattamenti in cui uno o più dei fattori o criteri suddetti sono presenti ma non si ritiene necessario procedere alla DPIA. Si veda la tabella seguente:

Esempi di trattamento	**Possibili criteri pertinenti**	**È probabile che sia richiesta una valutazione d'impatto sulla protezione dei dati?**
Un ospedale che tratta i dati genetici e sanitari dei propri pazienti (sistema informativo ospedaliero).	- Dati sensibili o dati aventi carattere estremamente personale. - Dati riguardanti soggetti interessati vulnerabili. - Trattamento di dati su larga scala.	Sì
L'uso di un sistema di telecamere per monitorare il comportamento di guida sulle autostrade. Il titolare del trattamento prevede di utilizzare un sistema intelligente di analisi video per individuare le auto e riconoscere automaticamente le targhe.	- Monitoraggio sistematico. - Uso innovativo o applicazione di soluzioni tecnologiche od organizzative.	
Un'azienda che monitora sistematicamente le attività dei suoi dipendenti, controllando anche la postazione di lavoro dei dipendenti, le loro attività in Internet, ecc.	- Monitoraggio sistematico. - Dati riguardanti soggetti interessati vulnerabili.	

La raccolta di dati pubblici dei media sociali per la generazione di profili.	- Valutazione o assegnazione di un punteggio. - Trattamento di dati su larga scala. - Creazione di corrispondenze o combinazione di insiemi di dati. - Dati sensibili o dati aventi carattere estremamente personale.	
Un'istituzione che crea una banca dati antifrode e di gestione del rating del credito a livello nazionale.	- Valutazione o assegnazione di un punteggio. - Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente. - Impedisce agli interessati di esercitare un diritto o utilizzare un servizio o un contratto. - Dati sensibili o dati aventi carattere estremamente personale.	
Conservazione per finalità di archiviazione di dati sensibili personali pseudonimizzati relativi a interessati vulnerabili coinvolti in progetti di ricerca o sperimentazioni cliniche.	- Dati sensibili. - Dati riguardanti soggetti interessati vulnerabili. - Impedisce agli interessati di esercitare un diritto o utilizzare un servizio o un contratto.	
Un trattamento di "dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato" (considerando 91).	- Dati sensibili o dati aventi carattere estremamente personale. - Dati riguardanti soggetti interessati vulnerabili.	
Una rivista online che utilizza una lista di distribuzione per inviare una selezione quotidiana generica ai suoi abbonati.	- Trattamento di dati su larga scala.	No

Un sito web di commercio elettronico che visualizza annunci pubblicitari per parti di auto d'epoca che comporta una limitata profilazione basata sugli articoli visualizzati o acquistati sul proprio sito web.	- Valutazione o assegnazione di un punteggio.	

Metodologie per la conduzione di una DPIA

Gli obiettivi di una DPIA sono i seguenti:

i) **Individuare** con precisione i rischi (elevati) che si associano al trattamento che ci si prefigge di realizzare, tenendo conto della natura dei dati e del trattamento, dell'ambito, del contesto e degli scopi del trattamento stesso, e delle fonti di rischio – non soltanto in circostanze normali, ma anche in situazioni speciali, nel breve, medio e lungo termine;[352]

ii) **Valutare** i rischi (elevati) previamente individuati, in particolare le fonti, la natura e le peculiarità, e la probabilità nonché l'eventuale gravità del rischio stesso;[353]

iii) Individuare quali **misure** adottare per mitigare i rischi (elevati), adeguate in termini di tecnologie disponibili e costi di implementazione, e propore tali misure[354]; e

iv) **Documentare** i risultati, le valutazioni e le misure adottate (o non adottate, e le relative motivazioni), in modo da poter "**dimostrare la conformità**" ai requisiti fissati nel RGPD in base al principio di "responsabilizzazione" con riguardo al trattamento in questione.[355]

L'Art. 35, paragrafo 6, del Regolamento prevede che (la documentazione de) la DPIA contenga "almeno" quanto segue:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e

[352] V. considerando 90 RGPD.
[353] V. considerando 84 RGPD e norma ISO 31000.
[354] V. considerando 84 RGPD.
[355] Per citare il WP29, "Una DPIA è un processo finalizzato a garantire e dimostrare la conformità" - Linee-guida del WP29 sulla DPIA. Per ulteriori informazioni sul principio di responsabilizzazione e gli obblighi derivanti di "dimostrazione della conformità", si veda la Parte II del Manuale.

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Il WP29 sottolinea che:

> Tutti i requisiti pertinenti stabiliti nel regolamento generale sulla protezione dei dati offrono un quadro ampio e generico per la progettazione e lo svolgimento di una valutazione d'impatto sulla protezione dei dati. L'attuazione pratica di una valutazione d'impatto sulla protezione dei dati dipenderà dai requisiti stabiliti nel regolamento generale sulla protezione dei dati che possono essere integrati da orientamenti pratici più dettagliati. **L'attuazione della valutazione d'impatto sulla protezione dei dati è quindi modulabile. Ciò significa che anche un titolare del trattamento di piccole dimensioni può progettare e attuare una valutazione d'impatto sulla protezione dei dati adatta ai propri trattamenti.**

Pertanto, i titolari possono, consultandosi con il proprio RPD, individuare una metodologia per qualsiasi DPIA debbano eventualmente condurre che sia adatta allo specifico contesto di attività. Possono fare affidamento sull'esperienza raccolta in occasione di valutazioni del rischio di natura più tecnica, per esempio effettuate sulla base della norma ISO 31000. Tuttavia, il WP29 evidenzia, correttamente, la diversa prospettiva in cui si collocano le valutazioni di impatto ai sensi del RGPD rispetto a quelle basate sulle norme ISO (comunque orientate in modo più restrittivo alle questioni di sicurezza):

> (…) la valutazione d'impatto sulla protezione dei dati svolta ai sensi del regolamento generale sulla protezione dei dati è uno strumento per gestire i rischi per i diritti degli interessati, di conseguenza, adotta la loro prospettiva, come avviene in taluni settori (ad esempio, la sicurezza sociale). Al contrario, la gestione del rischio in altri settori (ad esempio in quello della sicurezza delle informazioni) è incentrata sull'organizzazione.

Il WP29 menziona vari esempi di metodologie per la valutazione di impatto sulla protezione dei dati messe a punto dalle autorità nazionali di controllo,[356] e "incoraggia lo sviluppo di quadri di valutazione d'impatto specifici dei singoli settori". Ha, del resto, pubblicato una propria Griglia per le valutazioni di impatto riferite alle applicazioni RFID e un Modello di valutazione di impatto per le griglie intelligenti e i sistemi di contatori intelligenti.[357]

In questa sede ci limiteremo a riprodurre i Criteri per una DPIA accettabile fissati nelle Linee-guida del WP29:

Allegato 2 – Criteri per una valutazione di impatto sulla protezione dei dati accettabile

Il WP29 propone i seguenti criteri che i titolari del trattamento possono utilizzare per stabilire se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno oppure se una

[356] Si veda l'elenco comprendente legami ipertestuali pubblicato nell'Allegato 1 alle Linee-guida del WP29 sulla DPIA.
[357] Si veda l'Allegato 1 sopra menzionato e le relative note a piè di pagina, per maggiori riferimenti.

metodologia per lo svolgimento di una tale valutazione sia sufficientemente completa per garantire il rispetto del regolamento generale sulla protezione dei dati:

- **una descrizione sistematica del trattamento è fornita (articolo 35, paragrafo 7, lettera a)):**
    - la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono presi in considerazione (considerando 90);
    - vengono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali;
    - viene fornita una descrizione funzionale del trattamento;
    - sono individuate le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea);
    - si tiene conto del rispetto dei codici di condotta approvati (articolo 35, paragrafo 8);
- **la necessità e la proporzionalità sono valutate (articolo 35, paragrafo 7, lettera b)):**
    - sono state determinate le misure previste per garantire il rispetto del regolamento (articolo 35, paragrafo 7, lettera d) e considerando 90):
        - misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:
            - finalità determinate, esplicite e legittime (articolo 5, paragrafo 1, lettera b));
            - liceità del trattamento (articolo 6);
            - dati personali adeguati, pertinenti e limitati a quanto necessario (articolo 5, paragrafo 1, lettera c));
            - limitazione della conservazione (articolo 5, paragrafo 1, lettera e));
        - misure che contribuiscono ai diritti degli interessati:
            - informazioni fornite all'interessato (articoli 12, 13 e 14);
            - diritto di accesso e portabilità dei dati (articoli 15 e 20);
            - diritto di rettifica e alla cancellazione (articoli 16, 17 e 19);
            - diritto di opposizione e di limitazione di trattamento (articoli 18, 19 e 21);
            - rapporti con i responsabili del trattamento (articolo 28);
            - garanzie riguardanti trattamenti internazionali (capo V);
            - consultazione preventiva (articolo 36).
- **i rischi per i diritti e le libertà degli interessati sono gestiti (articolo 35, paragrafo 7 lettera c)):**

- l'origine, la natura, la particolarità e la gravità dei rischi (cfr. considerando 84) o, più in particolare, per ciascun rischio (accesso illegittimo, modifica indesiderata e scomparsa dei dati) vengono determinate dalla prospettiva degli interessati:
  - si considerano le fonti di rischio (considerando 90);
  - sono individuati gli impatti potenziali per i diritti e le libertà degli interessati in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati;
  - sono individuate minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati;
  - sono stimate la probabilità e la gravità (considerando 90);
- sono determinate le misure previste per gestire tali rischi (articolo 35, paragrafo 7, lettera d) e considerando 90);

- **le parti interessate sono coinvolte:**
  - si consulta il responsabile della protezione dei dati (articolo 35, paragrafo 2);
  - si raccolgono le opinioni degli interessati o dei loro rappresentanti, ove opportuno (articolo 35, paragrafo 9).

Come gestire la documentazione della DPIA

Il primo, nonché più importante, obiettivo della documentazione relativa a una DPIA (che soddisfi tutti i "criteri" sopra indicati) è quello di **dimostrare** la conduzione di una DPIA adeguata e approfondita, nel rispetto del RGPD (ossia, nel rispetto dei criteri sopra ricordati).

Ove la DPIA individui sia rischi (elevati), sia le misure adottabili per gestire tali rischi, che siano "adeguate" alla luce della probabilità e gravità dei rischi e dei costi delle misure stesse, e ove tali misure siano state effettivamente approvate e adottate (e anche di tale approvazione e adozione si abbia documentazione), la documentazione della DPIA può costituire un "elemento" importante ai fini della dimostrazione complessiva della conformità, nonché uno "strumento speciale" per raggiungere tale obiettivo (anche se non configura una presunzione assoluta di conformità in termini giuridici, e anche se il RPD dovrà comunque **verificare e monitorare**, su base continuativa, che le misure così individuate siano applicate e restino adeguate alla luce degli sviluppi organizzativi, tecnologici o applicativi: si veda, *infra*, il Compito successivo alla voce "Monitoraggio continuo della conformità").

Esempi di DPIA che hanno permesso di identificare rischi elevati e misure di mitigazione del rischio, ritenute sufficienti (nel caso specifico, dal consorzio EuroPrise) a consentire il trattamento. In entrambi gli esempi, pertanto, il titolare potrebbe giungere alla fondata conclusione che l'esito della DPIA mostra la NON necessità di sottoporre il trattamento per consultazione alla competente autorità di controllo.[358]

[358] Esempi tratti da prodotti che hanno ottenuto lo "European Privacy Seal", la cui valutazione giuridica è stata condotta da Douwe Korff. Si veda, rispettivamente:

1. **Un'agenzia di welfare utilizza l'autenticazione vocale per contrastare le frodi**

Identificazione dei rischi: come evidenziato dal WP29, tre dei principali rischi connessi all'impiego dei dati biometrici sono: (i) il fatto che le caratteristiche biometriche di una persona siano insostituibili (il che significa che un tool di autenticazione basato su dati biometrici grezzi non può essere sostituito una volta che i dati siano andati perduti); (ii) la facilità di utilizzo dei dati biometrici per confrontare diversi insiemi di dati; e (iii) la possibilità di raccogliere i dati biometrici all'insaputa dell'interessato.

Misure di mitigazione: In un tool di autenticazione biometrica (vocale), utilizzato per contrastare possibili frodi, si utilizza un template (modello) vocale univoco, creato dai dati biometrici ("grezzi") originali, anziché i dati grezzi veri e propri, che sono invece distrutti una volta arruolati gli interessati (cioè una volta raccolti i dati degli interessati). Il template vocale è univoco qualunque sia la specifica applicazione, e non può essere utilizzato per ricreare i dati biometrici (grezzi) originali. Ciò permette di gestire tutti i tre rischi sopra menzionati: (i) se il template vocale fosse compromesso, è possibile ricostituirne uno e diverso con grande facilità (con l'aiuto dell'interessato, che dovrebbe sottoporsi nuovamente al processo di arruolamento); (ii) i diversi template vocali utilizzati nelle singole applicazioni dello stesso tool non sono combinabili reciprocamente né con altri dati o template vocali; (iii) il template vocale viene creato durante un processo di arruolamento in presenza dell'interessato.

2. **Un'istituzione finanziaria verifica la posizione del cellulare di un cliente per stabilire se essa coincida (approssimativamente) con quella della carta bancaria del cliente (in quel momento utilizzata per compiere un'operazione segnalata come sospetta)**

Identificazione dei rischi: Informazioni sulla precisa posizione spaziale di una persona in un momento determinato possono rivelare dati estremamente sensibili, e la rivelazione di tali dati costituisce, pertanto, una grave ingerenza nella vita privata e nella riservatezza della persona interessata – come confermato dalla Corte europea dei diritti umani nel caso Naomi Campbell.

Misure di mitigazione: Nel tool progettato per la prevenzione di frodi nell'utilizzo di carte bancarie, i dati relativi all'ubicazione del cellulare vengono minimizzati, anche prima di essere trasferiti all'utilizzatore del tool (l'istituto finanziario), limitandoli a un'area molto ampia (una provincia, o uno Stato). Ciò è sufficiente per consentire un'efficiente operatività del tool, ossia per consentirgli di stabilire con sufficiente certezza se l'operazione in questione sia fraudolenta o reale, riducendo al tempo stesso l'invasività della verifica dell'ubicazione al minimo possibile.

https://www.european-privacy-seal.eu/EPS-en/4F-self-certification (un tool di autenticazione a quattro fattori che prevede una soluzione biometrica basata su registrazioni vocali);
https://www.european-privacy-seal.eu/eps-en/valid-pos (un tool che confronta la localizzazione di un'operazione bancaria sospetta effettuata con carte di credito con la localizzazione (approssimativa) del cellulare detenuto dal titolare della carta).
Nella valutazione, entrambi i prodotti sono stati giudicati molto positivamente per l'ampia minimizzazione dei dati e il ricorso a tecniche di privacy by design, nonché per i meccanismi con cui le due metodiche suddette riuscivano a mitigare, rispettivamente, i rischi associati all'impiego di dati biometrici e alle tecniche di tracciamento dell'ubicazione.

La documentazione può essere messa a disposizione (o utilizzata come termine di riferimento) in caso di **consultazioni** che coinvolgano le parti interessate o i cittadini, oppure per rispondere a **quesiti e reclami degli interessati e di ONG** che rappresentino gli interesssati (oppure della stampa). Sul punto, il WP29 osserva quanto segue:

> **La pubblicazione di una valutazione d'impatto sulla protezione dei dati non è un requisito giuridico sancito dal regolamento generale sulla protezione dei dati, è una decisione del titolari del trattamento procedere in tal senso. Tuttavia, i titolari del trattamento dovrebbero prendere in considerazione la pubblicazione di almeno alcune parti, ad esempio di una sintesi o della conclusione della loro valutazione d'impatto sulla protezione dei dati.**
>
> Lo scopo di un tale processo sarebbe quello di contribuire a stimolare la fiducia nei confronti dei trattamenti effettuati dal titolare del trattamento, nonché di dimostrare la responsabilizzazione e la trasparenza. ***Costituisce una prassi particolarmente buona pubblicare una valutazione d'impatto sulla protezione dei dati nel caso in cui individui della popolazione siano influenzati dal trattamento interessato. Nello specifico, ciò potrebbe essere il caso in cui un'autorità pubblica realizza una valutazione d'impatto sulla protezione dei dati***.
>
> La valutazione d'impatto sulla protezione dei dati pubblicata non deve necessariamente contenere l'intera valutazione, soprattutto qualora essa possa presentare informazioni specifiche relative ai rischi per la sicurezza per il titolare del trattamento o divulgare segreti commerciali o informazioni commerciali sensibili. In queste circostanze, la versione pubblicata potrebbe consistere soltanto in una sintesi delle principali risultanze della valutazione d'impatto sulla protezione dei dati o addirittura soltanto in una dichiarazione nella quale si afferma che la valutazione d'impatto sulla protezione dei dati è stata condotta.

La documentazione della DPIA assume particolare importanza in caso di richieste formulate da un'autorità di controllo, sia nell'ambito di attività generiche di vigilanza sia a seguito di reclami.

Più in particolare, qualora una DPIA identifichi sia rischi (elevati) sia l'assenza di misure adottabili per gestire in misura sufficiente tutti i rischi in questione (o almeno di misure "adeguate" alla luce della probabilità e gravità dei rischi e dei costi associati alle misure stesse), il titolare ha l'obbligo di **consultare l'autorità di controllo** (Art. 36), e **la documentazione della relativa DPIA deve essere fornita all'autorità di controllo**:

> (…) laddove una valutazione d'impatto sulla protezione dei dati riveli la presenza di rischi residui elevati, il titolare del trattamento sarà tenuto a richiedere la consultazione preventiva dell'autorità di controllo in relazione al trattamento (articolo 36, paragrafo 1). In tale contesto, la valutazione d'impatto sulla protezione dei dati deve essere fornita completa (articolo 36, paragrafo 3, lettera e)). L'autorità di controllo può fornire il proprio parere[359] e procurerà di non compromettere segreti commerciali né divulgare vulnerabilità di sicurezza, in conformità con i principi applicabili in ciascuno Stato membro in materia di accesso del pubblico a documenti ufficiali.

[359] Un parere in forma scritta rivolto al titolare è necessario solo se l'autorità di controllo ritiene che il trattamento previsto non sia conforme al Regolamento, secondo quqnto prevede l'Art. 36, paragrafo 2. [Nota originale nel testo]

Gli Stati membri possono anche prevedere per legge l'obbligo per i titolari di consultare l'autorità di controllo "in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica" (Art. 36, paragrafo 5) – e ciò è avvenuto, rispetto ai settori indicati, per esempio in Francia e in Italia.

Qualora l'autorità di controllo non sia soddisfatta delle informazioni contenute nella documentazione relativa alla DPIA, o comunque in altro modo fornite, può **ingiungere** al titolare di fornirle ogni altro elemento informativo che ritenga necessario per valutare la questione (v. Art. 58, paragrafo 1, lettera a)).

Generalmente l'autorità di controllo cercherà di **aiutare** il titolare nell'individuazione di una soluzione, ossia nell'individuazione di misure in grado di mitigare adeguatamente i rischi (elevati) già identificati (a parere dell'autorità stessa), e se il titolare accetta di applicare tali misure (e di garantire che la loro adozione e applicazione su base continuativa siano verificate e monitorate dall'RPD), la questione potrebbe chiudersi in tal modo (e di tutto ciò il RPD terrà traccia, come farà del resto la stessa autorità).

Tuttavia, l'autorità potrebbe anche **ingiungere** al titolare l'adozione di specifiche misure per il trattamento previsto (v. Art. 58, paragrafo 2, lettera d)), ovvero **vietare** il trattamento stesso (Art. 58, paragrafo 2, lettera f)).

Naturalmente, il RPD dovrà, ancora una volta, tenere traccia di ogni ingiunzione di questo tipo e verificare, su base continuativa, il rispetto delle prescrizioni impartite (documentando anche i risultati di tali verifiche). Tuttavia, a parte le verifiche in questione e l'attività di monitoraggio e documentazione, ogni responsabilità in caso di mancata osservanza ricadrà in ultima analisi sul titolare.

* * *

Controllo della conformità (comprese le indagini sui reclami)

COMPITO 5. Ripetizione dei Compiti 1 – 3 (e 4) su base continuativa

Come sottolineato dal WP29 nelle sue Linee guida sui RPD (approvate dal Comitato Europeo per la protezione dei dati – EDPB), l'Articolo 39(1)(b) affida al RPD l'incarico, fra gli altri compiti, di "controllare la conformità" della sua organizzazione al RGPD; il Considerando 97 specifica, inoltre, che il RPD "ha il compito di assistere il titolare o il responsabile nel monitoraggio interno della conformità al Regolamento".[360] Come indica il termine stesso di "monitoraggio", non si tratta di una responsabilità *una tantum*, ma di un compito su base continuativa.

Comunque, in linea con la discussione sul ruolo del RPD nella Parte 2, sezione 2.3.4, *supra*, il WP29 rileva (ulteriormente) che questo:[361]

> Non significa che la responsabilità, qualora si verifichi un caso di mancato rispetto, ricada personalmente sul RPD. Il RGPD stabilisce chiaramente che compete al titolare e non al RPD il compito di "attuare adeguate disposizioni *tecniche ed organizzative per garantire ed essere in grado di dimostrare che il trattamento viene eseguito in accordo con quanto stabilito dal Regolamento"* (Articolo 24(1)). La conformità della protezione dei dati è una responsabilità sociale del titolare del trattamento, e non del RPD.

Il WP29 prosegue affermando che, come parte dei compiti di controllo della conformità, il RPD ha, in particolare, il dovere di operare con continuità:

- nella raccolta di informazioni per identificare le attività di trattamento;
- nell'analisi e nel controllo della conformità delle attività di trattamento e
- nell'informazione, nell'attività di consulenza e di elaborazione di raccomandazioni destinate al titolare o al responsabile.

Come rilevato in relazione alla valutazione d'impatto della protezione dei dati - DPIA (Compito 4):[362]

> bisogna notare che per gestire il rischio ai diritti e alle libertà delle persone fisiche, i rischi devono essere identificati, analizzati, stimati, valutati, trattati (ed es., ridotti …), **e sottoposti a revisione periodica.**

In altre parole, i Compiti 1 – 4, supra (o, se non vi siano operazioni che possono comportare un "rischio elevato", i Compiti 1 – 3), vanno ripetuti su base continuativa, in particolare e soprattutto qualora l'organizzazione modifichi qualsiasi operazione di trattamento dei dati personali o ne adotti di nuove. Come afferma il GEPD (nel suo parere ai RPD delle Istituzioni e degli Organismi comunitari):[363]

> I vostri resoconti devono riflettere la realtà delle operazioni di trattamento [della vostra istituzione]. Questo significa che dovete garantirne l'aggiornamento. Quando [la vostra istituzione] pianifica delle modifiche alle vostre operazioni di trattamento dovete controllare se i resoconti devono essere aggiornati. É una buona idea che questo

---

360 Linee guida del WP29 sui RPD, sezione 4.1, *Controllo della conformità al RGPD*, p. 167.

361 *Idem*, originale in corsivo.

362 Linee guida del WP29 sulla Valutazione d'impatto della protezione dei dati - DPIA, nota 10 pagina 6, corsivo aggiunto.

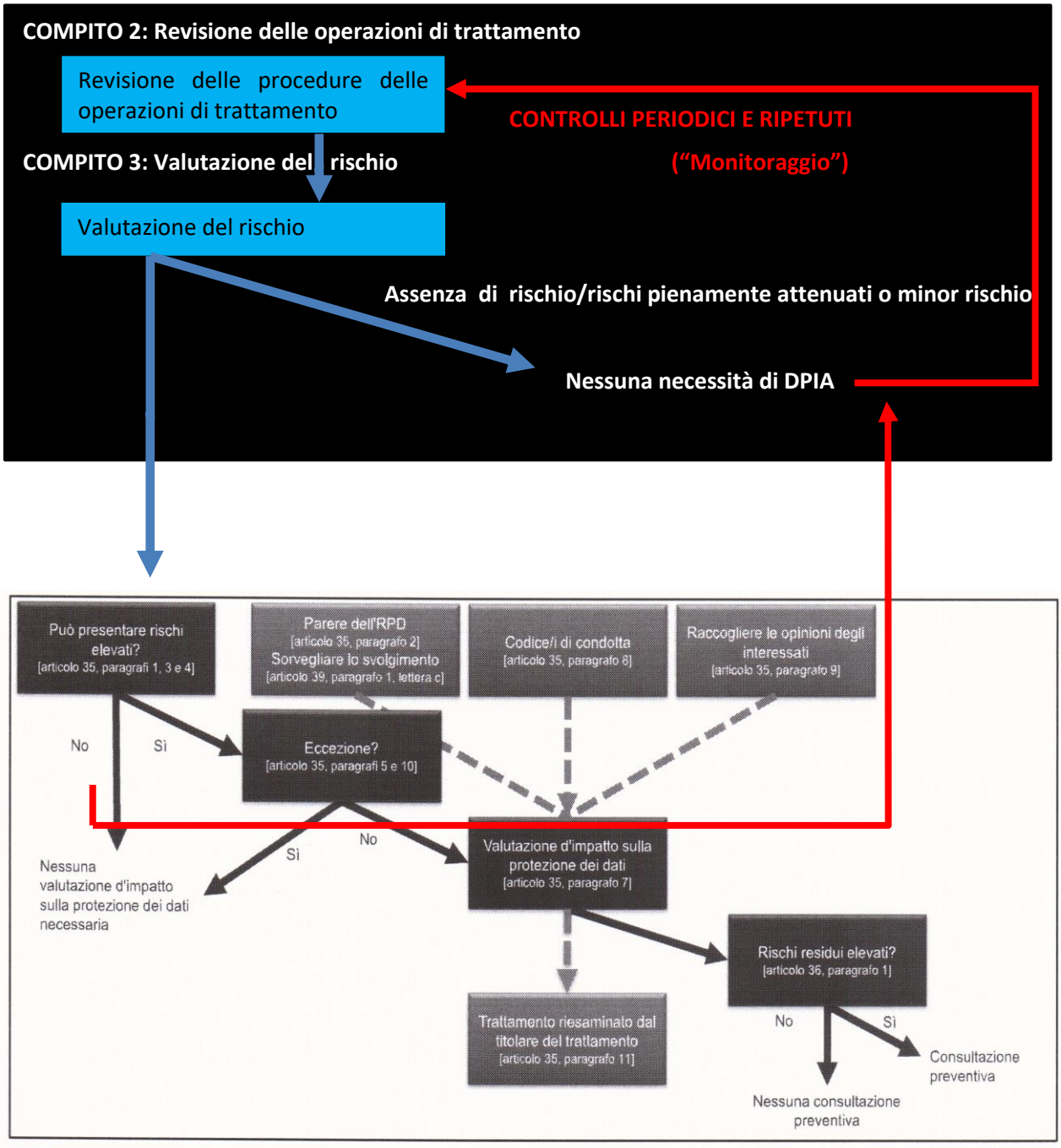
363 GEPD, (Accountability on the ground) (nota 297, *supra*).

controllo faccia formalmente parte del processo di "gestione del cambiamento" (change management). Potrebbe anche essere una buona idea effettuare revisioni su base regolare indipendentemente dai cambiamenti pianificati per cogliere quei cambiamenti che potrebbero passare inosservati.

Il WP29 ha illustrato l'ultima parte di questa sequenza in un diagramma molto utile, riportato di seguito, e che include l'aggiunta delle fasi previe (Compiti 2 e 3).

Diagramma del WP29 sulle tappe della procedura da compiere nella valutazione d'impatto della protezione dei dati - DPIA,[364] comprese le fasi previe (Compiti 2 e 3) che figurano nella parte alta del grafico:

[364] Linee guida del WP29 sulla valutazione d'impatto della protezione dei dati - DPIA, p. 7.



Nota: le eccezioni di cui all'Art. 35(5), riprese nel diagramma del WP29, fanno riferimento alla sicurezza nazionale, alla difesa, alla prevenzione della criminalità, ecc. L'Art. 35(10) riguarda la clausola per cui non è necessaria alcuna DPIA per un trattamento regolamentato a norma di legge se una DPIA generale di quel trattamento è stata eseguita nel quadro del processo legislativo (il che non riguarda il RPD).

Come parte dei suoi doveri di "monitoraggio della conformità", il RPD deve anche essere a conoscenza dei cambiamenti intervenuti nel quadro normativo, contrattuale, ecc. in cui opera la sua organizzazione, come disposto nei compiti preliminari (Compito 0), allo scopo di identificare l'impatto di tali cambiamenti (costante legittimità e conformità al RGPD) sui

trattamenti di dati personali della sua organizzazione e poter formulare raccomandazioni pertinenti destinate ai responsabili dell'organizzazione (comprese le alte dirigenze, se del caso).

Il RPD deve inoltre – se necessario e in collaborazione con altri RPD della rete dei RPD e/o con l'Autorità di controllo e in accordo con le alte dirigenze – essere pronto ad adottare posizioni o punti di vista sui cambiamenti suggeriti al quadro normativo e generale di cui sopra, ad esempio proposte avanzate dal governo sull'opportunità che l'organizzazione per la quale lavora debba richiedere, rendere possibile o incoraggiare la condivisione di determinati dati personali pernuove finalità.

- o – O – o –

COMPITO 6. Gestione delle violazioni dei dati personali

Due degli aspetti più importanti e innovativi contenuti nel RGPD rispetto alla Direttiva sulla Protezione dei dati personali del 1995 sono (i) un requisito generale di notifica alla DPA di riferimento (leggasi "competente") di ogni violazione dei dati personali che possa ingenerare rischi per i diritti e le libertà dei singoli e (ii) un dovere di informazione dell'interessato su queste violazioni qualora la violazione possa comportare un "rischio elevato" per i diritti e le libertà della persona fisica.

Il Gruppo di lavoro Articolo 29 (WP29) ha elaborato linee guida molto dettagliate su come debbano essere gestite le violazioni dei dati personali;[365] questo documento guida è stato approvato dal Comitato Europeo per la protezione dei dati (EDPB) nella sua prima riunione. La discussione che ci accingiamo ad affrontare farà ampiamente riferimento a queste linee guida e gli esempi citati provengono tutti da questo testo elaborato dal WP29. [366]

Notifica alla competente autorità di protezione dei dati o DPA

L'idea di notificare le violazioni dei dati personali non è nuova. Come visto alla sezione 1.3.3, *supra*,[367] un dovere di notifica della violazione dei dati personali figura già della Direttiva e-Privacy. Si trattava, tuttavia, di un obbligo limitato ai fornitori di reti e di servizi di comunicazioni elettroniche.[368] Il RGPD utilizza la stessa definizione di "*violazione dei dati personali*" come figura nella Direttiva e-Privacy, ma senza questa limitazione:

> la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. (Art. 4(12))[369]

Le Linee guida del WP29 chiariscono approfonditamente come i rispettivi termini debbano essere interpretati nel loro significato e specificano le diverse tipologie di violazione dei dati personali ("*violazione della riservatezza"; "violazione dell'integrità"; "violazione della disponibilità"*)[370]

Esempi

Un esempio di perdita di dati personali può essere la perdita o il furto di un dispositivo contenente una copia della banca dati dei clienti del titolare del trattamento. Un altro esempio può essere il caso in cui l'unica copia di un insieme di dati personali sia stata

---

365 Linee guida sulla notifica di violazione dei dati personali ai sensi del Regolamento 2016/679 del WP29 (WP250 rev.01, adottato il 3 ottobre 2017, revisione definitiva adottata il 6 Febbraio 2018 (cui faremo di seguito riferimento come: " Linee guida sulla notifica della violazione dei dati del WP29" o, in questa sezione e più semplicemente, "Linee guida del WP29" disponibili all'indirizzo: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

366 Le Linee guida del WP29 trattano anche degli obblighi di notifica nel quadro di altri strumenti giuridici: si veda la Sezione VI delle Linee guida. Questi argomenti non vengono ulteriormente affrontati qui.

367 Si veda la sotto-sezione relativa alle "*Caratteristiche principali del Regolamento e-Privacy*", sottorubrica "Notifica della violazione dei dati".

368 Come si sottolinea nella parte introduttiva delle Linee guida del WP29, alcuni Stati membri hanno già provveduto ad ampliare i requisiti di notifica della violazione dei dati personali.

369 La Direttiva e-Privacy aggiunge a questo dettato le parole: "*nel contesto di servizi di comunicazione accessibili al pubblico nella Comunità*" (art. 2(i)).

370 Linee guida del WP29, p. 7, con riferimento ad un precedente Parere (2014) del WP29 sulla notifica della violazione.

crittografata da un *ransomware* (*malware* del riscatto) oppure dal titolare del trattamento mediante una chiave non più in suo possesso.

Fra gli esempi di perdita della disponibilità dei dati rientrano la cancellazione accidentale, la cancellazione operata da una persona non autorizzata o, nell'esempio testé citato di dati criptati in modo sicuro, la perdita della chiave di crittografia. Qualora il titolare non possa ripristinare l'accesso ai dati, tramite, ad esempio, un backup, ci troviamo di fronte ad una perdita permanente di disponibilità.

Una perdita di disponibilità si può anche registrare anche per una grave interruzione nel normale funzionamento di una fornitura di servizio, pensiamo ad un black-out energetico o a un attacco del tipo "diniego di servizio" che rendono impossibile la disponibilità dei dati personali.

Anche una perdita temporanea di disponibilità può costituire una violazione dei dati personali:

Esempi

In ambito ospedaliero, se i dati clinici cruciali di un paziente risultano non disponibili, anche solo momentaneamente, questa situazione può mettere a rischio i diritti e le libertà del singolo; un intervento chirurgico, ad esempio, può essere cancellato a rischio della vita.

Al contrario, nel caso di un'azienda del settore dei media, i cui servizi sono interrotti per molte ore per un black-out elettrico, se all'azienda viene impedito di mandare una comunicazione agli abbonati su quanto accaduto è improbabile che questo costituisca un rischio per i diritti e le libertà dei singoli.

Un'infezione da ransomware può determinare una perdita temporanea di disponibilità, se i dati possono essere ripristinati dal backup. Trattandosi, comunque, di un'intrusione nella rete, potrebbe essere necessaria una notifica se l'incidente viene qualificato come violazione della riservatezza (ad esempio, accesso ai dati personali da parte dell'aggressore della rete) e , inoltre, si tratta di un caso di specie che mette a rischio i diritti e le libertà del singolo.

L'Articolo 33(1) sancisce che:

> In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo (Articolo 33(1)).

Il responsabile del trattamento deve "*informare il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione*" (Art. 33(2)). Il WP29 raccomanda che il responsabile:

> Notifichi **prontamente** al titolare e fornisca ogni ulteriore informazione sulla violazione mano a mano che i dettagli si rendono disponibili. Questo è un aspetto importante per mettere il titolare nelle condizioni di rispettare l'obbligo di notifica all'autorità di controllo entro 72 ore (Linee guida del WP29, pag. 14).

Il titolare viene considerato "**a conoscenza**" della violazione una volta messo al corrente dal responsabile;[371] il titolare deve allora notificare l'accaduto all'Autorità della protezione dei dati - DPA (come ricordato), a meno si applichi il *caveat* relativo all'improbabilità che la violazione dei dati comporti un rischio per i diritti e le libertà individuali.

In alcuni casi, un responsabile può agire per un certo di un certo numero, anche cospicuo, di titolari diversi, pensiamo al fornitore di servizi di conservazione dei dati su cloud. Il WP29, in questi casi, formula il seguente parere:

> laddove il responsabile fornisca servizi a più titolari tutti implicati nello stesso incidente, il responsabile avrà il compito di segnalare i dettagli dell'incidente a ciascun titolare.
>
> Il responsabile deve effettuare una notifica per conto del titolare se il titolare ha fornito al responsabile apposita autorizzazione e se questo è previsto dagli accordi contrattuali fra titolare e responsabile. Tale notifica deve essere redatta ai sensi degli Articoli 33 e 34. É comunque importante rilevare che la responsabilità giuridica della notifica ricade sul titolare (p.14).

La notifica della violazione dei dati alla DPA competente[372] "deve almeno":

> a. descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
>
> b. comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
>
> c. descrivere le probabili conseguenze della violazione dei dati personali;
>
> d. descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
>
> (Art. 33(3))

A tal proposito, il WP29 afferma che il titolare può:[373]

> se necessario, sceglier di fornire ulteriori dettagli. Alcuni tipi di violazione (riservatezza, integrità o disponibilità) possono richiedere informazioni aggiuntive per spiegare appieno le circostanze in cui i fatti si sono verificati.

Esempio

Nell'ambito della notifica all'autorità di controllo, il titolare del trattamento può ritenere utile indicare il nome del responsabile del trattamento, qualora quest'ultimo sia la causa di fondo della violazione, in particolare se quest'ultima ha provocato un incidente ai danni delle registrazioni dei dati personali di molti altri titolari del trattamento che fanno ricorso al medesimo responsabile del trattamento.

---

371 Linee guida del WP29, pag. 14.

372 Per informazioni sulla notifica di violazioni transfrontaliere e violazioni che si sono verificate all'esterno degli organismi dell'UE, si veda la Sezione C delle Linee guida del WP29 (pp. 16 – 18).

373 Linee guida del WP29, pag. 15.

Durante le indagini sulla violazione, l'autorità di controllo può comunque richiedere dettagli ulteriori.

Inoltre:

qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo (Art. 33(4)).[374]

Esempio

Un titolare del trattamento notifica all'autorità di controllo entro 72 ore l'individuazione di una violazione derivante dalla perdita di una chiave USB contenente una copia dei dati personali di alcuni dei suoi clienti. In seguito scopre che la chiave USB non era stata messa al suo posto e la recupera. Il titolare del trattamento aggiorna l'autorità di controllo e chiede la modifica della notifica.

Termini per la notifica

Le Linee guida del WP29 chiariscono quando un titolare (o un responsabile) può venire considerato "**a conoscenza**" della violazione dei dati e sottolineano che vanno rispettati una serie di obblighi per anticipare e preparare una simile evenienza:[375]

Come indicato in precedenza, il regolamento impone al titolare del trattamento di notificare una violazione senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza. Questo solleva la questione relativa al momento in cui il titolare del trattamento può considerarsi "a conoscenza" di una violazione. Il Gruppo di lavoro ritiene che il titolare del trattamento debba considerarsi "a conoscenza" nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali.

Tuttavia, come già osservato, il regolamento impone al titolare del trattamento di attuare tutte le misure tecniche e organizzative di protezione adeguate per stabilire immediatamente se si è verificata una violazione e informare tempestivamente l'autorità di controllo e gli interessati. Afferma altresì che è opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione e delle sue conseguenze e dei suoi effetti negativi per l'interessato[376]. Il titolare del trattamento è quindi tenuto a prendere le misure necessarie per assicurarsi di venire "a conoscenza" di eventuali violazioni in maniera tempestiva in modo da poter adottare le misure appropriate.

Il momento esatto in cui il titolare del trattamento può considerarsi "a conoscenza" di una particolare violazione dipenderà dalle circostanze della violazione. In alcuni casi sarà relativamente evidente fin dall'inizio che c'è stata una violazione, mentre in altri potrebbe occorrere del tempo per stabilire se i dati personali sono stati compromessi. Tuttavia, l'accento dovrebbe essere posto sulla tempestività dell'azione per indagare su un incidente per stabilire se i dati personali sono stati effettivamente violati e, in caso affermativo, prendere misure correttive ed effettuare la notifica, se necessario.

Esempi

374 Per dettagli ed ulteriori informazioni su questo problema si vedano le Linee guida del WP29, pp. 15 – 16.

375 Linee guida del WP29, pp. 10 – 11.

376 Cfr. Considerando 87.

1. In caso di perdita di una chiave USB contenente dati personali non crittografati spesso non è possibile accertare se persone non autorizzate abbiano avuto accesso ai dati. Tuttavia, anche se il titolare del trattamento non è in grado di stabilire se si è verificata una violazione della riservatezza, tale caso deve essere notificato, in quanto sussiste una ragionevole certezza del fatto che si è verificata una violazione della disponibilità; il titolare del trattamento si considera venuto "a conoscenza" della violazione nel momento in cui si è accorto di aver perso la chiave USB.

2. Un terzo informa il titolare del trattamento di aver ricevuto accidentalmente i dati personali di uno dei suoi clienti e fornisce la prova della divulgazione non autorizzata. Dato che al titolare del trattamento è stata presentata una prova evidente di una violazione della riservatezza, non vi è dubbio che ne sia venuto "a conoscenza".

3. Un titolare del trattamento rileva che c'è stata una possibile intrusione nella sua rete. Controlla quindi i propri sistemi per stabilire se i dati personali ivi presenti sono stati compromessi e ne ottiene conferma. Ancora una volta, dato che il titolare del trattamento ha una chiara prova di una violazione non può esserci dubbio che sia venuto "a conoscenza" della stessa.

4. Un criminale informatico viola il sistema del titolare del trattamento e lo contatta per chiedere un riscatto. In tal caso, dopo aver verificato il suo sistema per accertarsi dell'attacco, il titolare del trattamento dispone di prove evidenti che si è verificata una violazione e non vi è dubbio che ne sia venuto a conoscenza.

5. Una persona informa il titolare del trattamento di aver ricevuto un'e-mail da un soggetto che si fa passare per il titolare del trattamento, contenente dati personali relativi al suo (effettivo) utilizzo del servizio del titolare del trattamento, aspetto questo che suggerisce che la sicurezza del titolare del trattamento sia stata compromessa. Il titolare del trattamento conduce una breve indagine e individua un'intrusione nella propria rete e la prova di un accesso non autorizzato ai dati personali. Il titolare del trattamento si considera "a conoscenza" della violazione in questo momento e dovrà procedere alla notifica all'autorità di controllo a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Il titolare del trattamento dovrà prendere le opportune misure correttive per far fronte alla violazione.

Documentazione e valutazione della violazione

Il RGPD sancisce che:

> Il titolare del trattamento documenta **qualsiasi** violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo. (Art. 33(5), neretto aggiunto)

Va rilevato che quest'ultimo requisito fa riferimento a **tutte** le violazioni di dati personali e non si limita, pertanto, a quelle che devono essere oggetto di notifica alle Autorità di supervisione; devono essere registrate anche tutte le violazioni che (secondo il titolare) "è improbabile comportino un rischio ai diritti e alle libertà delle persone fisiche".

In pratica, il RPD deve essere coinvolto seriamente e da vicino in queste problematiche. É probabile che una sospetta violazione sia denunciata internamente spesso proprio a lui (e/o al Responsabile tecnologia o al Responsabile sicurezza) e per questo il RPD (con l'ausilio di

questi responsabili, se necessario) ha il compito di una prima ed immediata valutazione (almeno) dei seguenti elementi:

- se vi è stata violazione dei dati personali ai sensi del RGPD (si veda la definizione di cui all'Articolo 4(12) citato *supra*), *ve ne siano le prove o è probabile/possibile che si tratti di una violazione;*
- quali categorie di persone interessate sono state o possono essere state oggetto di violazione e quali categorie di dati personali possono essere andati persi o sono interessati dalla violazione;

  NB: il WP29 raccomanda che queste categorie figurino in ogni notifica di violazione destinata all'Autorità di supervisione e soprattutto che:[377]

  > se i tipi di interessati o di dati personali rivelano un rischio di danno particolare a seguito di una violazione (ad esempio usurpazione d'identità, frode, perdite finanziarie, minaccia al segreto professionale) è importante che la notifica indichi tali categorie. In questo modo, l'obbligo di descrivere le categorie si collega all'obbligo di descriverne le probabili conseguenze della violazione

  e, tenuto conto di questi elementi,
- se la violazione comporta un rischio "probabile" o "improbabile" di mettere in pericolo i diritti e le libertà delle persone fisiche.

  Il WP29 discute dettagliatamente il problema di quando la notifica non sia necessaria[378] e cita il seguente esempio:

> **Esempio**
>
> Una violazione che non richiederebbe la notifica all'autorità di controllo sarebbe la perdita di un dispositivo mobile crittografato in maniera sicura, utilizzato dal titolare del trattamento e dal suo personale. Se la chiave di cifratura rimane in possesso del titolare del trattamento e non si tratta dell'unica copia dei dati personali, questi ultimi sarebbero inaccessibili a qualsiasi pirata informatico. Ciò significa che è improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati in questione. Se in seguito diventa evidente che la chiave di cifratura è stata compromessa o che il software o l'algoritmo di cifratura è vulnerabile, il rischio per i diritti e le libertà delle persone fisiche cambia e potrebbe quindi essere necessaria la notifica.

*Se la valutazione è tale da confermare che **esiste** un rischio potenziale di tal genere:*

- valutare se il rischio è "elevato per i diritti e le libertà delle persone fisiche" (perché questo implicherebbe non solo la notifica della violazione all'Autorità competente, ma anche il darne informazione ai soggetti interessati, come vedremo nella prossima sottorubrica).[379]

---

377 Linee guida del WP29, pag. 14.

378 Linee guida del WP29, pp. 18 – 19. Si veda anche la lista, non esaustiva, di esempi di cui all'Allegato B delle Linee guida riprodotto *infra* alla successiva sottorubrica.

379 Si veda, nello specifico, la discussione alla sottorubrica *"Valutazione del rischio e rischio elevato"*.

Come sottolinea il WP29, l'importanza di essere in grado di identificare una violazione, valutare il rischio per gli interessati e notificarla se necessario figura al Considerando 87 del RGPD:

> É opportuno verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato. È opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato. Siffatta notifica può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento.

Naturalmente, se la valutazione indica che violazione vi è stata e che vi sono rischi per gli interessi delle persone fisiche, è necessario provvedere con urgenza a **misure di mitigazione dei rischi**.

Il problema deve essere segnalato **tempestivamente e urgentemente** ai più alti livelli dirigenziali. Non appena sia accertata l'esistenza di una violazione, nessuna discussione interna deve rallentare il coinvolgimento dei vertici dell'organizzazione.

É necessaria **un'attenta e scrupolosa registrazione**[380] delle valutazioni eseguite, dei risultati e delle motivazioni delle stesse; delle misure di contenimento attuate; della comunicazione ai vertici delle valutazioni e delle misure proposte; delle misure autorizzate (se e quando) dalla dirigenza; del fatto che la violazione (qualora notificabile) sia stata notificata all'Autorità per la protezione dei dati (DPA) di riferimento e quando (con copia della notifica); e, ove necessario, dell'informazione data agli interessati, con copia della relativa notifica e di eventuali comunicati stampa, ecc., come vedremo nel prossimo capitolo. Inoltre, come sottolineano le Linee guida del WP29:

> la violazione dovrebbe essere documentata durante tutta la sua evoluzione (p. 12).

Nelle organizzazioni che hanno nominato un RPD, questa figura gioca un ruolo importante in un caso come questo, come messo in rilievo dal WP29:[381]

> Il titolare del trattamento o il responsabile del trattamento può avere un responsabile della protezione dei dati[382], come richiesto dall'articolo 37 oppure su decisione volontaria come buona prassi. L'articolo 39 del regolamento stabilisce una serie di compiti obbligatori per il responsabile della protezione dei dati, ma non impedisce l'assegnazione di ulteriori compiti da parte del titolare del trattamento, se del caso.
>
> Tra i compiti obbligatori del responsabile della protezione dei dati di particolare rilevanza per la notifica delle violazioni figurano quelli di fornire consulenza e informazioni al titolare del trattamento o al responsabile del trattamento, sorvegliare l'osservanza del regolamento e fornire un parere in merito alle valutazioni d'impatto sulla protezione dei dati. Il responsabile della protezione dei dati deve inoltre cooperare con l'autorità di controllo e fungere da punto di contatto per l'autorità di controllo e

---

380 Il WP29 suggerisce che le registrazioni figurino "*nel piano di segnalazione delle violazioni del titolare e/o negli accordi di organizzazione interna*" (p. 12). Ulteriori dettagli si ritrovano nelle Linee guida del WP29, Sezione V, *"Responsabilizzazione e tenuta dei registri*".

381 Linee guida del WP29, Sezione V. B, pp. 27 – 28.

382 Cfr. le Linee guida del Gruppo di lavoro sui Responsabili della Protezione dei Dati: https://www.garanteprivacy.it/documents/10160/0/WP+243+-+Linee-guida+sui+responsabili+della+protezione+dei+dati+%28RPD%29.pdf.

> per gli interessati. Va inoltre osservato che, ai fini della notifica della violazione all'autorità di controllo, l'articolo 33, paragrafo 3, lettera b), impone al titolare del trattamento di fornire il nome e i dati di contatto del responsabile della protezione dei dati o di un altro punto di contatto.
>
> Per quanto riguarda la documentazione delle violazioni, il titolare del trattamento o il responsabile del trattamento potrebbe chiedere il parere del proprio responsabile della protezione dei dati in merito alla struttura, all'impostazione e all'amministrazione della documentazione. Al responsabile della protezione dei dati potrebbe altresì essere affidato il compito di tenere i registri.
>
> Questi compiti indicano che il responsabile della protezione dei dati dovrebbe svolgere un ruolo chiave nel fornire assistenza nella prevenzione delle violazioni o nella preparazione alle stesse, fornendo consulenza e monitorando il rispetto delle norme, nonché durante una violazione (ossia nel processo di notifica all'autorità di controllo) e durante qualsiasi successiva indagine da parte dell'autorità di controllo. In tale ottica, il Gruppo di lavoro raccomanda di informare tempestivamente il responsabile della protezione dei dati dell'esistenza di una violazione e di coinvolgerlo nella gestione delle violazioni e nel processo di notifica.

Le Linee guida del WP29 stabiliscono chiaramente che le organizzazioni non solo hanno il compito di reagire in situazioni simili, ma devono anche dotarsi di **politiche di sicurezza** che prevengano **in anticipo** ogni violazione dei dati e di piani atti a prevenire, limitare e mettere fine ad ogni violazione. Per quanto riguarda le attività di elaborazione dei dati personali che possono comportare un "rischio elevato" per le persone fisiche, la definizione di queste politiche costituirebbe un elemento importante di una valutazione d'impatto sulla protezione dei dati (come discusso per il compito 4, *supra*).[383]

Comunicazioni all'interessato

Le Linee guida del WP29 chiariscono nei seguenti termini i requisiti per comunicare la violazione dei dati alle persone fisiche interessate:

> In alcuni casi, oltre a effettuare la notifica all'autorità di controllo, il titolare del trattamento è tenuto a comunicare la violazione alle persone fisiche interessate.
>
> L'Articolo 34(1) stabilisce che:
>
> > Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo".
>
> Il titolare del trattamento dovrebbe tenere a mente che la notifica all'autorità di controllo è obbligatoria a meno che sia improbabile che dalla violazione possano derivare rischi per i diritti e le libertà delle persone fisiche. Inoltre, laddove la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche occorre informare anche queste ultime. La soglia per la comunicazione delle violazioni alle persone fisiche è quindi più elevata rispetto a quella della notifica alle autorità di controllo, pertanto non tutte le violazioni dovranno essere comunicate agli interessati, il che li protegge da inutili disturbi arrecati dalla notifica.
>
> Il regolamento afferma che la comunicazione di una violazione agli interessati dovrebbe avvenire "senza ingiustificato ritardo", il che significa il prima possibile. L'obiettivo

383 Linee guida del WP29, pag. 6.

> principale della comunicazione agli interessati consiste nel fornire loro informazioni specifiche sulle misure che questi possono prendere per proteggersi[384]. Come osservato in precedenza, a seconda della natura della violazione e del rischio presentato, la comunicazione tempestiva aiuterà le persone a prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

Un allegato (Allegato B) alle Linee guida del WP29 con una lista (non esaustiva) di 10 esempi di violazioni di dati personali con obbligo di notifica figura quale documento al presente compito sotto la dicitura Allegato.

Le Linee guida del WP29 proseguono citando le:[385]

> **Informazioni da fornire**
>
> Ai fini della comunicazione alle persone fisiche, l'Articolo 34(2) specifica che:
>
> > La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d) dell'Articolo 33(3).
>
> Secondo tale disposizione, il titolare del trattamento deve fornire almeno le seguenti informazioni:
>
> - una descrizione della natura della violazione;
> - il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto;
> - una descrizione delle probabili conseguenze della violazione;
> - una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

Esempio:

Come esempio di misure adottate per far fronte alla violazione e attenuarne i possibili effetti negativi, il titolare del trattamento può dichiarare che, dopo aver notificato la violazione all'autorità di controllo pertinente, ha ricevuto consigli sulla gestione della violazione e sull'attenuazione del suo impatto. Se del caso, il titolare del trattamento dovrebbe anche fornire consulenza specifica alle persone fisiche sul modo in cui proteggersi dalle possibili conseguenze negative della violazione, ad esempio reimpostando le password in caso di compromissione delle credenziali di accesso. Ancora una volta, il titolare del trattamento può scegliere di fornire informazioni supplementari rispetto a quanto richiesto qui.

Le Linee guida chiariscono che:[386]

> in linea di principio, la violazione dovrebbe essere comunicata direttamente agli interessati coinvolti, a meno che ciò richieda uno sforzo sproporzionato. In tal caso, si

384 Cfr. anche il Considerando 86.

385 Sezione III. B, pag. 20.

386 Sezione III. C, pag. 21; si veda questa sezione sulle modalità alternative di comunicare una violazione dei dati che pregiudica gli interessati.

> procede a una comunicazione pubblica o a una misura simile che permetta di informare gli interessati con analoga efficacia (Articolo 34(3)c).

Le comunicazioni agli interessati dovrebbero essere effettuate "non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo" (Considerando 86). Come evidenziano le linee-guida:[387]

> il titolare del trattamento potrebbe quindi contattare e consultare l'autorità di controllo non soltanto per chiedere consiglio sull'opportunità di informare gli interessati in merito a una violazione ai sensi dell'articolo 34, ma anche sui messaggi appropriati da inviare loro e sul modo più opportuno per contattarli.
>
> Parallelamente, il Considerando 88 indica che la notifica di una violazione dovrebbe tenere "conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali". Ciò può significare che in determinate circostanze, ove giustificato e su consiglio delle autorità incaricate dell'applicazione della legge, il titolare del trattamento può ritardare la comunicazione della violazione agli interessati fino a quando la comunicazione non pregiudica più tale indagine. Tuttavia, passato tale arco di tempo, gli interessati dovrebbero comunque essere tempestivamente informati.
>
> Se non ha la possibilità di comunicare una violazione all'interessato perché non dispone di dati sufficienti per contattarlo, il titolare del trattamento dovrebbe informarlo non appena sia ragionevolmente possibile farlo (ad esempio quando l'interessato esercita il proprio diritto ai sensi dell'articolo 15 di accedere ai dati personali e fornisce al titolare del trattamento le informazioni supplementari necessarie per essere contattato).

Eccezioni

Come rilevano le Linee guida del WP29:[388]

> L'articolo 34, paragrafo 3, stabilisce tre condizioni che, se soddisfatte, non richiedono la comunicazione agli interessati in caso di violazione, ossia:
>
> - Il titolare del trattamento ha applicato misure tecniche e organizzative adeguate per proteggere i dati personali prima della violazione, in particolare misure atte a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi. Ciò potrebbe prevedere ad esempio la protezione dei dati personali con cifratura allo stato dell'arte oppure mediante tokenizzazione;
> - Immediatamente dopo una violazione, il titolare del trattamento ha adottato misure destinate a garantire che non sia più probabile che si concretizzi l'elevato rischio posto ai diritti e alle libertà delle persone fisiche. Ad esempio, a seconda delle circostanze del caso, il titolare del trattamento può aver immediatamente individuato e intrapreso un'azione contro il soggetto che ha avuto accesso ai dati personali prima che questi fosse in grado di utilizzarli in qualsiasi modo. È necessario altresì tenere in debito conto delle possibili conseguenze di qualsiasi violazione della riservatezza, anche in questo caso, a seconda della natura dei dati in questione;

---

387 *Idem*, pp. 21 – 22.

388 Sezione III. D, pag. 22, sono stati omessi i riferimenti alle note.

- contattare gli interessati richiederebbe uno sforzo sproporzionato[389], ad esempio nel caso in cui i dati di contatto siano stati persi a causa della violazione o non siano mai stati noti. Si pensi, ad esempio, al magazzino di un ufficio statistico che si è allagato e i documenti contenenti dati personali erano conservati soltanto in formato cartaceo. In tale circostanza il titolare del trattamento deve invece effettuare una comunicazione pubblica o prendere una misura analoga, tramite la quale gli interessati vengano informati in maniera altrettanto efficace. In caso di sforzo sproporzionato, si potrebbe altresì prevedere l'adozione di disposizioni tecniche per rendere le informazioni sulla violazione disponibili su richiesta, soluzione questa che potrebbe rivelarsi utile per le persone fisiche che potrebbero essere interessate da una violazione ma che il titolare del trattamento non può altrimenti contattare.

Conformemente al principio di responsabilizzazione, il titolare del trattamento dovrebbe essere in grado di dimostrare all'autorità di controllo di soddisfare una o più di queste condizioni[390].Va tenuto presente che, sebbene la comunicazione possa inizialmente non essere richiesta se non vi è alcun rischio per i diritti e le libertà delle persone fisiche, la situazione potrebbe cambiare nel corso del tempo e il rischio dovrebbe essere rivalutato.

Se il titolare del trattamento decide di non comunicare una violazione all'interessato, l'articolo 34(4), spiega che l'autorità di controllo può richiedere che lo faccia, qualora ritenga che la violazione possa presentare un rischio elevato per l'interessato. In alternativa, può ritenere che siano state soddisfatte le condizioni di cui all'articolo 34(3), nel qual caso la comunicazione all'interessato non è richiesta. Qualora stabilisca che la decisione di non effettuare la comunicazione all'interessato non sia fondata, l'autorità di controllo può prendere in considerazione l'esercizio dei poteri e delle sanzioni a sua disposizione.

Valutazione dell'esistenza di un rischio e di un rischio elevato

Ancora una volta può essere sufficiente citare le Linee guida del WP29:[391]

> Sebbene il regolamento introduca l'obbligo di notificare una violazione, non è obbligatorio farlo in tutte le circostanze:
>
> - la notifica all'autorità di controllo competente è obbligatoria a meno che sia improbabile che la violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche;
> - la comunicazione di una violazione alle persone fisiche diventa necessaria soltanto laddove la violazione possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
>
> Ciò significa che non appena il titolare del trattamento viene a conoscenza di una violazione, è fondamentale che non si limiti a contenere l'incidente, ma valuti anche il rischio che potrebbe derivarne. Questo per due motivi: innanzitutto conoscere la probabilità e la potenziale gravità dell'impatto sulle persone fisiche aiuterà il titolare del trattamento ad adottare misure efficaci per contenere e risolvere la violazione; in secondo luogo, ciò lo aiuterà a stabilire se è necessaria la notifica all'autorità di controllo e, se necessario, alle persone fisiche interessate.

[389] Cfr. le Linee guida del Gruppo di lavoro sulla trasparenza con riguardo alla natura sproporzionata dello sforzo. Il testo è disponibile (in inglese) all'indirizzo: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850.
[390] Cfr. Articolo 5, paragrafo 2.
[391] Sezione IV. A e B, pag. 23, riferimenti omessi.

Come spiegato in precedenza, la notifica di una violazione è obbligatoria a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche, mentre la comunicazione di una violazione agli interessati deve essere effettuata se è probabile che la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche. Tale rischio sussiste quando la violazione può comportare un danno fisico, materiale o immateriale per le persone fisiche i cui dati sono stati violati.

Esempi:

Esempi di tali danni sono la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie e il pregiudizio alla reputazione. Il verificarsi di tale danno dovrebbe essere considerato probabile quando la violazione riguarda dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, oppure che includono dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza.

Fattori da considerare nella valutazione del rischio

I Considerando 75 e 76 del regolamento suggeriscono che, di norma, nella valutazione del rischio si dovrebbero prendere in considerazione tanto la probabilità quanto la gravità del rischio per i diritti e le libertà degli interessati. Inoltre il regolamento afferma che il rischio dovrebbe essere valutato in base a una valutazione oggettiva.

Va osservato che la valutazione del rischio per i diritti e le libertà delle persone fisiche a seguito di una violazione esamina il rischio in maniera diversa rispetto alla valutazione d'impatto sulla protezione dei dati[392]. Quest'ultima considera tanto i rischi del trattamento dei dati svolto come pianificato, quanto quelli in caso di violazione. Nel considerare una potenziale violazione, esamina in termini generali la probabilità che la stessa si verifichi e il danno all'interessato che potrebbe derivarne; in altre parole, si tratta di una valutazione di un evento ipotetico. Nel caso di una violazione effettiva, l'evento si è già verificato, quindi l'attenzione si concentra esclusivamente sul rischio risultante dell'impatto di tale violazione sulle persone fisiche.

Esempio:
La valutazione d'impatto sulla protezione dei dati (DPIA) suggerisce che l'uso proposto di un determinato software di sicurezza per proteggere i dati personali costituisce una misura adeguata per garantire un livello di sicurezza adeguato al rischio che il trattamento presenterebbe altrimenti per le persone fisiche. Tuttavia, laddove una vulnerabilità diventi nota successivamente, ciò modifica l'idoneità del software a contenere il rischio per i dati personali protetti e richiede quindi una rivalutazione nel contesto di una valutazione d'impatto come parte integrante di una DPIA su base continua.

Una vulnerabilità nel prodotto viene sfruttata in un secondo momento e si verifica una violazione. Il titolare del trattamento dovrebbe valutare le circostanze specifiche della violazione, i dati interessati e il potenziale livello di impatto sulle persone fisiche, nonché la probabilità che tale rischio si concretizzi.

[392]Cfr. le Linee guida del Gruppo di lavoro in materia di valutazione d'impatto sulla protezione dei dati: https://www.garanteprivacy.it/documents/10160/0/WP+248+-+Linee-guida+concernenti+valutazione+impatto+sulla+protezione+dati.

Di conseguenza, nel valutare il rischio per le persone fisiche derivante da una violazione, il titolare del trattamento dovrebbe considerare le circostanze specifiche della violazione, inclusa la gravità dell'impatto potenziale e la probabilità che tale impatto si verifichi. Pertanto il Gruppo di lavoro 29 raccomanda che la valutazione tenga conto dei seguenti criteri:[393]

Tipo di violazione

Il tipo di violazione verificatosi può influire sul livello di rischio presentato per le persone fisiche.

Esempio:

Ad esempio, una violazione della riservatezza che ha portato alla divulgazione di informazioni mediche a soggetti non autorizzati può avere conseguenze diverse per una persona fisica rispetto a una violazione in cui i dettagli medici di una persona fisica sono stati persi e non sono più disponibili.

Natura, carattere sensibile e volume dei dati personali

Ovviamente, un elemento fondamentale della valutazione del rischio sono il tipo e il carattere sensibile dei dati personali che sono stati compromessi dalla violazione. Solitamente più i dati sono sensibili, maggiore è il rischio di danni per le persone interessate; tuttavia si dovrebbero prendere in considerazione anche altri dati personali che potrebbero già essere disponibili sull'interessato. Ad esempio, è improbabile che la divulgazione del nome e dell'indirizzo di una persona fisica in circostanze ordinarie causi un danno sostanziale. Tuttavia, se il nome e l'indirizzo di un genitore adottivo sono divulgati a un genitore biologico, le conseguenze potrebbero essere molto gravi tanto per il genitore adottivo quanto per il bambino.

Violazioni relative a dati sulla salute, documenti di identità o dati finanziari come i dettagli di carte di credito, possono tutte causare danni di per sé, ma se tali dati fossero usati congiuntamente si potrebbe avere un'usurpazione d'identità. Di norma una combinazione di dati personali ha un carattere più sensibile rispetto a un singolo dato personale.

Alcuni tipi di dati personali possono sembrare relativamente innocui, tuttavia occorre valutare attentamente ciò che questi dati possono rivelare sull'interessato. Un elenco di clienti che accettano consegne regolari potrebbe non essere particolarmente sensibile, tuttavia gli stessi dati relativi a clienti che hanno richiesto l'interruzione delle loro consegne durante le vacanze potrebbero essere informazioni utili per dei criminali.

Analogamente, una piccola quantità di dati personali altamente sensibili può avere un impatto notevole su una persona fisica, mentre una vasta gamma di dettagli può rivelare molte più informazioni in merito alla stessa persona. Inoltre, una violazione che interessa grandi quantità di dati personali relative a molte persone può avere ripercussioni su un numero corrispondentemente elevato di persone.

Facilità di identificazione delle persone fisiche

Un fattore importante da considerare è la facilità con cui un soggetto che può accedere a dati personali compromessi riesce a identificare persone specifiche o ad abbinare i

[393] L'Articolo 3.2 del Regolamento 611/2013 enumera i fattori che dovrebbero essere tenuti in considerazione in relazione alla notifica di violazioni nei settori di servizi di comunicazione elettronica, un riferimento che potrebbe essere utile nel contesto della notifica ai sensi del RGPD. Si veda: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF [nota originale]

dati con altre informazioni per identificare persone fisiche. A seconda delle circostanze, l'identificazione potrebbe essere possibile direttamente dai dati personali oggetto di violazione senza che sia necessaria alcuna ricerca speciale per scoprire l'identità dell'interessato, oppure potrebbe essere estremamente difficile abbinare i dati personali a una particolare persona fisica, ma sarebbe comunque possibile a determinate condizioni. L'identificazione può essere direttamente o indirettamente possibile a partire dai dati oggetto di violazione, tuttavia può dipendere anche dal contesto specifico della violazione e dalla disponibilità pubblica dei corrispondenti dettagli personali. Quest'ultima eventualità potrebbe essere più rilevante per le violazioni della riservatezza e della disponibilità.

Come indicato in precedenza, i dati personali protetti da un livello appropriato di cifratura saranno incomprensibili a persone non autorizzate che non dispongono della chiave di decifratura. Inoltre, anche una pseudonimizzazione opportunamente attuata (definita all'articolo 4 (5), come "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile") può ridurre la probabilità che le persone fisiche vengano identificate in caso di violazione. Tuttavia, le tecniche di pseudonimizzazione da sole non possono essere considerate sufficienti a rendere i dati incomprensibili

Gravità delle conseguenze per le persone fisiche

A seconda della natura dei dati personali coinvolti in una violazione, ad esempio categorie particolari di dati, il danno potenziale alle persone che potrebbe derivarne può essere particolarmente grave soprattutto se la violazione può comportare furto o usurpazione di identità, danni fisici, disagio psicologico, umiliazione o danni alla reputazione. Se la violazione riguarda dati personali relativi a persone fisiche vulnerabili, queste ultime potrebbero essere esposte a un rischio maggiore di danni.

Il fatto che il titolare del trattamento sappia o meno che i dati personali sono nelle mani di persone le cui intenzioni sono sconosciute o potenzialmente dannose può incidere sul livello di rischio potenziale. Prendiamo una violazione della riservatezza nel cui ambito i dati personali vengono comunicati a un terzo di cui all'articolo 4, punto 10, o ad altri destinatari per errore. Una tale situazione può verificarsi, ad esempio, nel caso in cui i dati personali vengano inviati accidentalmente all'ufficio sbagliato di un'organizzazione o a un'organizzazione fornitrice utilizzata frequentemente. Il titolare del trattamento può chiedere al destinatario di restituire o distruggere in maniera sicura i dati ricevuti. In entrambi i casi, dato che il titolare del trattamento ha una relazione continuativa con tali soggetti e potrebbe essere a conoscenza delle loro procedure, della loro storia e di altri dettagli pertinenti, il destinatario può essere considerato "affidabile". In altre parole, il titolare del trattamento può ritenere che il destinatario goda di una certa affidabilità e può ragionevolmente aspettarsi che non leggerà o accederà ai dati inviati per errore e che rispetterà le istruzioni di restituirli. Anche se i dati fossero stati consultati, il titolare del trattamento potrebbe comunque confidare nel fatto che il destinatario non intraprenderà ulteriori azioni in merito agli stessi e restituirà tempestivamente i dati al titolare del trattamento e coopererà per garantirne il recupero. In tali casi, questo aspetto può essere preso in considerazione nella valutazione del rischio effettuata dal titolare del trattamento in seguito alla violazione; il fatto che il destinatario sia affidabile può neutralizzare la gravità delle conseguenze della violazione, anche se questo non significa che non si sia verificata una violazione. La probabilità che detta violazione presenti un rischio per le persone fisiche verrebbe

però meno, quindi non sarebbe più necessaria la notifica all'autorità di controllo o alle persone fisiche interessate. Ancora una volta, tutto dipenderà dalle circostanze del caso concreto. Ciò nonostante il titolare del trattamento deve comunque conservare informazioni relative alla violazione nel contesto del suo dovere generale di conservare registrazioni in merito alle violazioni (…).

Si dovrebbe altresì tener conto della permanenza delle conseguenze per le persone fisiche, per cui l'impatto può essere considerato maggiore qualora gli effetti siano a lungo termine.

Caratteristiche particolari dell'interessato

Una violazione può riguardare dati personali relativi a minori o ad altre persone fisiche vulnerabili, che possono di conseguenza essere soggette a un rischio più elevato di danno. Altri fattori concernenti la persona fisica potrebbero influire sul livello di impatto della violazione sulla stessa.

Caratteristiche particolari del titolare del trattamento dei dati

La natura e il ruolo del titolare del trattamento e delle sue attività possono influire sul livello di rischio per le persone fisiche in seguito a una violazione. Ad esempio, un'organizzazione medica tratterà categorie particolari di dati personali, il che significa che vi è una minaccia maggiore per le persone fisiche nel caso in cui i loro dati personali vengano violati, rispetto a una mailing list di un quotidiano.

Numero di persone fisiche interessate

Una violazione può riguardare solo una o poche persone fisiche oppure diverse migliaia di persone fisiche, se non molte di più. Di norma, maggiore è il numero di persone fisiche interessate, maggiore è l'impatto che una violazione può avere. Tuttavia, una violazione può avere ripercussioni gravi anche su una sola persona fisica, a seconda della natura dei dati personali e del contesto nel quale i dati sono stati compromessi. Ancora una volta, l'aspetto fondamentale consiste nel considerare la probabilità e la gravità dell'impatto sulle persone interessate.

Aspetti generali

Pertanto, nel valutare il rischio che potrebbe derivare da una violazione, il titolare del trattamento dovrebbe considerare tanto la gravità dell'impatto potenziale sui diritti e sulle libertà delle persone fisiche quanto la probabilità che tale impatto si verifichi. Chiaramente, se le conseguenze di una violazione sono più gravi, il rischio è più elevato; analogamente, se la probabilità che tali conseguenze si verifichino è maggiore, maggiore è anche il rischio. In caso di dubbio, il titolare del trattamento dovrebbe restare molto prudente ed effettuare la notifica. L'allegato B fornisce alcuni esempi utili di diversi tipi di violazioni che comportano rischi o rischi elevati per le persone fisiche.

L'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) ha elaborato raccomandazioni in merito a una metodologia di valutazione della gravità di una violazione, che possono essere utili per i titolari del trattamento e i responsabili del trattamento nella progettazione del loro piano di risposta per la gestione delle violazioni.[394]

- o – O – o -

[394] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, https://www.enisa.europa.eu/publications/dbn-severity [nota originale].

Allegato:

Esempi di violazioni di dati personali e dei soggetti cui notificarli (dalle Linee guida del WP29)

Esempio	**Notifica all'autorità di controllo?**	**Comunicazione all'interessato?**	**Note/raccomandazioni**
i. Un titolare del trattamento ha effettuato un backup di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata durante un'effrazione.	No.	No.	Fintantoché i dati sono crittografati con un algoritmo all'avanguardia, esistono backup dei dati, la chiave univoca non viene compromessa e i dati possono essere ripristinati in tempo utile, potrebbe non trattarsi di una violazione da segnalare. Tuttavia, se la chiave viene successivamente compromessa, è necessaria la notifica.
ii. Un titolare del trattamento gestisce un servizio online. A seguito di un attacco informatico ai danni di tale servizio, i dati personali di persone fisiche vengono prelevati. Il titolare del trattamento ha clienti in un solo Stato membro.	Sì, segnalare l'evento all'autorità di controllo se vi sono probabili conseguenze per le persone fisiche.	Sì, segnalare l'evento alle persone fisiche a seconda della natura dei dati personali interessati e se la gravità delle probabili conseguenze per tali persone è elevata.	
iii. Una breve interruzione di corrente di alcuni minuti presso il call center di un titolare del trattamento impedisce ai clienti di chiamare il titolare del trattamento e accedere alle proprie registrazioni.	No.	No.	Questa non è una violazione soggetta a notifica, ma costituisce comunque un incidente registrabile ai sensi dell'articolo 33(5). Il titolare del trattamento deve conservare adeguate registrazioni in merito.

iv. Un titolare del trattamento subisce un attacco tramite *ransomware* che provoca la cifratura di tutti i dati. Non sono disponibili backup e i dati non possono essere ripristinati. Durante le indagini, diventa evidente che l'unica funzionalità dal *ransomware* era la cifratura dei dati e che non vi erano altri *malware* presenti nel sistema.	Sì, effettuare la segnalazione all'autorità di controllo, se vi sono probabili conseguenze per le persone fisiche in quanto si tratta di una perdita di disponibilità.	Sì, effettuare la segnalazione alle persone fisiche, a seconda della natura dei dati personali interessati e del possibile effetto della mancanza di disponibilità dei dati, nonché di altre possibili conseguenze.	Se fosse stato disponibile un backup e i dati avessero potuto essere ripristinati in tempo utile non sarebbe stato necessario segnalare la violazione all'autorità di controllo o alle persone fisiche, in quanto non si sarebbe verificata nessuna perdita permanente di disponibilità o di riservatezza. Tuttavia, qualora l'autorità di controllo fosse venuta a conoscenza dell'incidente con altri mezzi, avrebbe potuto prendere in considerazione lo svolgimento di un'indagine al fine di valutare il rispetto dei requisiti di sicurezza più ampi di cui all'articolo 32.
v. Una persona telefona al call center di una banca per segnalare una violazione dei dati. La persona ha ricevuto l'estratto conto mensile da un soggetto diverso. Il titolare del trattamento intraprende una breve indagine (ossia la conclude entro 24 ore) e stabilisce con ragionevole certezza che si è verificata una violazione dei dati personali e che vi è una potenziale carenza sistemica che potrebbe comportare il coinvolgimento già occorso o potenziale	Si.	La comunicazione va effettuata soltanto alle persone fisiche coinvolte in caso di rischio elevato e se è evidente che altre persone fisiche non sono state interessate dall'evento.	Se dopo ulteriori indagini si stabilisce che l'evento ha interessato un numero maggiore di persone fisiche è necessario comunicare questo sviluppo all'autorità di controllo, e il titolare del trattamento deve informarne le altre persone fisiche interessate se sussiste un rischio elevato per loro.

di altre persone fisiche.			
vi. Un titolare del trattamento gestisce un mercato online e ha clienti in più Stati membri. Tale mercato subisce un attacco informatico a seguito del quale i nomi utente, le password e la cronologia degli acquisti vengono pubblicati online dall'autore dell'attacco.	Sì, segnalare l'evento all'autorità di controllo capofila se la violazione riguarda un trattamento transfrontaliero.	Sì, dato che la violazione potrebbe comportare un rischio elevato	Il titolare del trattamento dovrebbe prendere delle misure, ad esempio forzare il ripristino delle password degli account interessati, e altri provvedimenti per attenuare il rischio. Il titolare del trattamento dovrebbe altresì considerare qualsiasi altro obbligo di notifica, ad esempio ai sensi della direttiva NIS, trattandosi di un fornitore di servizi digitali.
vii. Una società di *hosting* di siti web che funge da responsabile del trattamento individua un errore nel codice che controlla l'autorizzazione dell'utente. A causa di tale vizio, qualsiasi utente può accedere ai dettagli dell'account di qualsiasi altro utente.	In veste di responsabile del trattamento, la società di *hosting* di siti web deve effettuare la notifica ai clienti interessati (i titolari del trattamento) senza ingiustificato ritardo. Supponendo che la società di *hosting* di siti web abbia condotto le proprie indagini, i titolari del trattamento interessati dovrebbero essere ragionevolmente certi di aver subito una violazione e pertanto è probabile che vengano considerati "a conoscenza" della violazione nel momento in cui hanno ricevuto la notifica da parte della società di *hosting* (il responsabile del trattamento). Il	Qualora non vi siano probabili rischi elevati per le persone fisiche non è necessario effettuare una comunicazione a tali persone.	La società di *hosting* di siti web (responsabile del trattamento) deve prendere in considerazione qualsiasi altro obbligo di notifica (ad esempio ai sensi della direttiva NIS, trattandosi di un fornitore di servizi digitali). Qualora non vi sia alcuna prova che tale vulnerabilità sia sfruttata presso uno dei suoi titolari del trattamento, la violazione potrebbe non essere soggetta all'obbligo di notifica, tuttavia potrebbe essere una violazione da registrare o essere il segno di un mancato rispetto dell'articolo 32.

	titolare del trattamento deve quindi effettuare la notifica all'autorità di controllo.		
viii. Le cartelle cliniche di un ospedale sono indisponibili per un periodo di 30 ore a causa di un attacco informatico.	Sì, l'ospedale è tenuto a effettuare la notifica in quanto può verificarsi un rischio elevato per la salute e la tutela della vita privata dei pazienti.	Sì, informare le persone fisiche coinvolte.	
ix. I dati personali di un gran numero di studenti vengono inviati per errore a una mailing list sbagliata con più di 1 000 destinatari.	Sì, segnalare l'evento all'autorità di controllo.	Sì, segnalare l'evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	
x. Una e-mail di marketing diretto viene inviata ai destinatari nei campi "a:" o "cc:", consentendo così a ciascun destinatario di vedere l'indirizzo e-mail di altri destinatari.	Sì, la notifica all'autorità di controllo può essere obbligatoria se è interessato un numero elevato di persone, se vengono rivelati dati sensibili (ad esempio una mailing list di uno psicoterapeuta) o se altri fattori presentano rischi elevati (ad esempio, il messaggio di posta elettronica contiene le password iniziali).	Sì, segnalare l'evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	La notifica potrebbe non essere necessaria se non vengono rivelati dati sensibili e se viene rivelato soltanto un numero limitato di indirizzi di posta elettronica.

- o – O – o -

COMPITO 7. Compiti di indagine (compresa la gestione dei reclami interni ed esterni)

Nota: Questo Compito è distinto e separato dalla gestione delle richieste di accesso, rettifica ecc. del soggetto interessato e di cui al Compito 8.

Indagine

Sebbene non se ne faccia esplicita menzione nel RGPD, il compito di indagine deriva dalla più ampia descrizione della posizione generale e delle mansioni del RPD – e in particolare dall'obbligo di "controllo della conformità" di cui al RGPD, Art. 39(1)(b) – secondo la quale il RPD, per iniziativa propria o su richiesta della dirigenza dell'organizzazione cui appartiene oppure, per esempio, del sindacato o dei rappresentanti del personale o ancora di una qualsiasi persona fisica (interna o esterna alla propria organizzazione, ma potremmo anche citare un informatore (*whistleblower*), che si spera goda delle opportune tutele nel paese interessato) ha l'incarico di **indagare** sulle questioni e i fatti direttamente collegati con l'esercizio delle proprie funzioni e **riferisce** alla persona o all'autorità che ha commissionato l'indagine o lo ha incaricato della stessa e/o alle alte dirigenze. Come ricorda il GEPD nel suo Documento di sintesi (Position Paper) sui RPD:[395]

> **Monitoraggio della conformità** (…): Il RPD ha il compito di garantire l'applicazione del Regolamento nella sua organizzazione. Il RPD, di propria iniziativa o su richiesta dell'organizzazione, del titolare, delle istanze del personale o di qualsiasi persona fisica ha l'incarico di indagare sulle questioni e i fatti direttamente collegati con l'esercizio delle proprie funzioni e riferisce alla persona o all'autorità che ha commissionato l'indagine o al titolare.

Il RGPD stabilisce chiaramente – anche se in termini meno espliciti dell'*Allegato* al Regolamento sulla protezione dei dati nelle Istituzioni dell'UE – che i RPD devono disporre di **tutte le risorse necessarie** e **dell'accesso a tutti i dati e tutti gli uffici, alle installazioni per il trattamento dei dati informatici e ai supporti di dati** (con tutti i poteri di ***autenticazione, accesso e conservazione***) necessari all'esecuzione dei loro compiti (cfr. Art. 38(2)), quindi anche all'espletamento di tali indagini.[396] Allo stesso modo, sebbene, ancora una volta, il dettato delle norme sia più esplicito per i RPD delle Istituzioni dell'UE che per quelli nominati ai sensi del RGPD, **tutto il personale del titolare della protezione dei dati – ma anche il personale di ogni agenzia esterna, e, in particolare, dei responsabili del trattamento (compresi i fornitori di servizi cloud utilizzati dal titolare) – devono dare piena assistenza al RPD nelle sue indagini**, e ***fornire risposte ed informazioni complete ed esaustive*** ad ogni interrogativo o richiesta del RPD.[397] **I titolari devono chiaramente far figurare queste disposizioni nelle norme destinate al personale interno e includerle nei contratti con fornitori esterni e responsabili del trattamento.**

---

395 GEPD, Documento di sintesi (Position paper) sul ruolo dei RPD nella garanzia di un'efficace conformità al Regolamento (CE) 45/2001 (nota 240, *supra*), p.6, testo originale in grassetto.

396 L'*Allegato* al Regolamento (UE) 45/2001 stabilisce che i RPD delle Istituzioni dell'UE: "*hanno accesso in qualsiasi momento ai dati oggetto del trattamento e a tutti gli uffici, alle installazioni per il trattamento dei dati e ai supporti di dati.*" (*Allegato*, articolo 4, secondo capoverso).

397 L'*Allegato* al Regolamento (UE) 45/2001 stabilisce che: "*Ogni responsabile del trattamento deve assistere il responsabile della protezione dei dati nell'esercizio delle sue funzioni e rispondere ai quesiti sottopostigli.*" (*Allegato*, Art. 4, primo capoverso).

Poteri esecutivi

Nonostante le competenze di cui al RGPD in materia di controllo della conformità, di gestione dei reclami e di indagine sulle possibili violazioni del Regolamento, il **RPD dispone solo di limitati poteri esecutivi**. In linea di principio, come rilevato precedentemente, se il RPD ritiene che la propria organizzazione (o un fornitore o un responsabile del trattamento) non abbia rispettato, per certi aspetti, le disposizioni del RGPD, è suo dovere riferire ai massimi vertici – cui incombe la responsabilità di azioni correttive, comprese, se del caso, sanzioni nei confronti di membri del personale, agenti, responsabili del trattamento venuti meno ai loro obblighi, azioni che possono andare da una segnalazione, ad un avvertimento o, per i casi più gravi, al licenziamento e alla rescissione del contratto. Ad esempio, se un fornitore di servizi esterni ha il compito di raccogliere dati (con un sistema automatico gestito dal fornitore stesso, per es.) e questo fornitore non si conforma al RGPD, non rispettando gli obblighi di informazione o, peggio, utilizzando surrettiziamente i dati raccolti per ulteriori (e non dichiarate) finalità, il RPD ha l'obbligo di proporre che il titolare cambi fornitore e deve, contemporaneamente, avvisare la DPA.

L'omissione di tali provvedimenti sarà imputata al titolare (l'organizzazione) nel quadro delle misure di esecuzione messe in atto dall'Autorità nazionale di protezione dei dati (DPA) anche per definire l'ammontare di ogni "sanzione amministrativa pecuniaria" (cfr. Art. 83).

Inoltre, uno dei compiti del RPD è quello di "consultare" la competente Autorità di controllo "laddove opportuno", relativamente a qualunque altra questione (Art. 39(1)(e)). Qualora emerga una seria divergenza di vedute fra il RPD e le alte dirigenze dell'organizzazione, e il RPD ritenga che uno specifico trattamento costituisca o possa costituire una violazione (significativa) del RGPD e/o delle disposizioni nazionali in materia, egli ha il dovere di esercitare il proprio potere e riferire la questione alla DPA (a maggior ragione nel caso in cui le dirigenze vogliano procedere comunque al trattamento o non intendano comminare sanzioni). A questo punto spetta alla DPA decidere se utilizzare le proprie ampie competenze di controllo e di indagine, inclusa la possibilità di imporre, se lo ritiene opportuno, una limitazione provvisoria (o definitiva) al trattamento o il divieto del trattamento stesso (si veda Art. 58(2)(d) e (f) in particolare).

Maggiori informazioni figurano, *infra*, ai capitoli "*Cooperazione e consultazione con la DPA*" e *"Trattamento di richieste e reclami*".

- o – O – o -

Funzioni consultive

COMPITO 8. Funzioni di consulenza – aspetti generali.

Il RPD deve garantire il rispetto del Regolamento e vigilare sull'osservanza degli obblighi dei titolari. Per questo motivo deve **informare**, **fornire** consulenza o elaborare **raccomandazioni** per il ***miglioramento pratico*** della protezione dei dati da parte dell'organizzazione e/o sulle questioni connesse all'applicazione delle disposizioni in materia di protezione dei dati (sia, ad esempio, quelle di cui al RGPD, sia quelle figuranti in altri testi legislativi dell'Ue – come la Direttiva e-Privacy del 2002 e, in futuro, il Regolamento e-Privacy – che quelle previste dalle legislazioni nazionali come elaborate sulla base delle clausole "di specificazione" del RGPD o comunque in vigore) e ***modificare ed aggiornare le prassi e le politiche dell'ente o dell'organismo in materia di protezione dei dati*** alla luce dei nuovi strumenti giuridici, delle decisioni, delle misure e delle linee guida adottate (cfr. Art. 39(1)(a)).

All'uopo, il RPD deve potere **seguire da vicino gli sviluppi normativi primari e secondari in materia di protezione dei dati, sicurezza dei dati, ecc.** e avvisare i livelli dirigenziali appropriati dell'elaborazione prossima di ***nuovi strumenti giuridici dell'UE*** (come il Regolamento e-Privacy cui facevamo riferimento prima); di nuove ***decisioni esecutive o giurisprudenziali europee*** (come ogni nuova "decisione sull'adeguatezza" da parte della Commissione Europea riguardante Paesi terzi verso i quali l'organizzazione del RPD trasferisce dati, oppure le sentenze della CGUE); ***di nuovi orientamenti dell'UE*** (in particolare pareri, raccomandazioni ecc. elaborati dal ***EDPB***) e di ***analoghi strumenti, decisioni, misure o linee guida elaborati nel paese (o nei paesi) dell'organizzazione del RPD.*** Il RGPD **stabilisce** che ogni titolare che si avvale di un RPD gli garantisca "***[tutte] le risorse necessarie*** *per assolvere tali compiti … e* ***mantenere la propria conoscenza specialistica***" (Art. 38(2)). Il RPD deve quindi avere la possibilità – ed essere incoraggiato – a partecipare a seminari, conferenze e riunioni, in particolare quelli organizzati dall'Autorità di protezione dei dati nazionale o regionale.

Il RPD **può anche essere consultato** dalla dirigenza, dagli organismi di rappresentanza del personale o dai sindacati interni, dagli stessi membri del personale, compresi, naturalmente, ogni "responsabile di attività" / ogni soggetto nell'organizzazione che abbia specifiche responsabilità con riguardo a specifici trattamenti e abbia bisogno di un consiglio; più in generale, **deve essere consultato** sui temi pertinenti (cfr. anche il Compito 7, di cui parleremo al prossimo capitolo).

Come enunciato dal WP29 nelle **Linee guida sui RPD** (poi formalmente recepite dal Comitato):[398]

> Ciò significa che l'organizzazione dovrà, per esempio, garantire:
>
> - che il RPD sia invitato a partecipare su base regolare alle riunioni del management di alto e medio livello;
> - che il RPD sia presente ogniqualvolta debbano essere raggiunte decisioni che impattano sulla protezione dei dati. Il RPD deve disporre tempestivamente di tutte le informazioni pertinenti in modo da poter rendere una consulenza idonea;
> - che il parere del RPD riceva sempre la dovuta considerazione. In caso di disaccordi, il Gruppo di lavoro raccomanda, quale buona prassi, di documentare le motivazioni che hanno portato a condotte difformi da quelle raccomandate dal RPD;

[398] Linee guida del WP29 sui RPD (nota 239, *supra*), pp. 13 – 14.

- che il RPD sia consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

Ove opportuno, il titolare del trattamento o il responsabile del trattamento potrebbero mettere a punto linee guida ovvero programmazioni in materia di protezione dei dati che indichino i casi di consultazione obbligatoria dei RPD.

- o – O – o -

COMPITO 9. Sostegno e promozione dei principi di "Protezione dei dati fin dalla progettazione e la Protezione dei dati per impostazione predefinita" (Data Protection by Design & Default).

Come rilevato nella discussione sul Compito 6, *supra*, il RPD deve essere consultato su qualunque tipo di problema relativo alla protezione dei dati che emerga nella propria organizzazione, compresa l'elaborazione di linee guida di politica generale, ecc.

Un problema di particolare rilevanza, in tal senso, è rappresentato dalla nuova ed esplicita disposizione del RGPD (non ancora enunciata nella Direttiva sulla protezione dei dati del 1995, sebbene già intuibile fra le righe)[399] che prevede che i titolari integrino il principio di "**Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita (data protection by design and by default)**" (che include anche quello di "***security by design [and default]***")[400] in tutte le loro attività. Come sancito nell'articolo 25:

> Articolo 25
>
> **Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita**
>
> 1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.
> 2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.
> 3. …[401]

Il principio può essere discusso qui solo brevemente. Il GEPD riassume il **concetto generale ed il contesto** come segue:[402]

---

399 Cfr., ad esempio, il reiterato riferimento a questo principio nel Parere 8/2014 sui recenti sviluppi dell'Internet delle cose del WP 29 (WP 223), adottato il 16 settembre 2014, all'indirizzo: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

400 Cfr. WP223 (nota precedente), p. 22, penultimo trattino.

401 Il terzo paragrafo stabilisce che: " *Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo*". Questo aspetto viene discusso in relazione al Compito 9, *infra*.

402 GEPD, Parere preliminare sulla "privacy by design" (Parere 5/2018), del 31 maggio 2018, p. 4, paragrafo 17 (originale in corsivo), all'indirizzo: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf (corsivo aggiunto)
Va rilevato che il GEPD opera un distinguo fra il principio, più ampio, di "privacy by design", portatore di una "dimensione visionaria ed etica", e quello più specificamente giuridico di "data protection by design" e "data

> Il termine "privacy by design" è stato usato per la prima volta da Ann Cavoukian quando era Commissario all'informazione e alla Privacy dell'Ontario, Canada. In questo concetto, la "privacy by design" può essere divisa in "**7 principi fondamentali**",[403] che sottolineano la necessità di un approccio **proattivo** nel considerare le esigenze di protezione della vita privata [o, nei termini usati dall'UE, la protezione dei dati] dalla fase di progettazione a tutto il ciclo di vita dei dati che devono essere *"integrati nella concezione e nell'architettura dei sistemi IT e delle prassi commerciali … senza diminuirne la funzionalità"* con il rispetto della privacy come parametro predefinito, la sicurezza end-to-end, compresa la sicurezza della distruzione dei dati, e una forte trasparenza subordinata ad una verifica indipendente. Il principio della "privacy by default" è stato definito come il secondo principio fondamentale, in base al quale un approccio di "privacy by design" deve *"garantire che i dati personali siano automaticamente protetti in ogni sistema informatico o in ogni prassi commerciale. Anche se il singolo non fa nulla, la sua vita privata è comunque protetta. Al singolo non è richiesta nessuna azione per proteggere la propria vita privata* – ***questa protezione è integrale al sistema, per impostazione predefinita"***. Questa dichiarazione è una definizione operativa potente del principio della "privacy by default", per cui la persona non è tenuta ad adoperarsi per proteggere la propria vita privata nell'utilizzo di un servizio o di un prodotto, ma beneficia « automaticamente » (perché non le è richiesto alcun comportamento attivo) del diritto fondamentale alla privacy e alla protezione dei dati personali.

Agli occhi del GEPD, la protezione dei dati "per impostazione predefinita" presenta **diverse dimensioni**; parafrasando il testo:[404]

- la **prima dimensione** è che le attività di trattamento dei dati personali devono sempre essere il ***risultato di un processo di concezione*** che copra ***l'intero ciclo di vita del progetto***, in cui devono figurare chiaramente la protezione delle persone e dei loro dati a carattere personale;
- la **seconda dimensione** riguarda il fatto che il processo di concezione si basi su un ***approccio alla gestione dei rischi*** per il quale i beni da proteggere sono ***le persone di cui vengono trattati i dati e, in particolare, le loro libertà e diritti fondamentali;***
- la **terza dimensione** riguarda il fatto che le misure da approntare per proteggere le persone, i loro diritti e le loro libertà devono essere ***appropriate ed efficaci*** in relazione a tali rischi, alla luce dei principi di protezione dei dati di cui all'Articolo 5 del RGPD che possono essere considerati ***obiettivi da raggiungere***;
- la **quarta dimensione** è ***l'obbligo di integrare al trattamento le garanzie e le salvaguardie definite [necessarie, appropriate ed effettive]***.

---

protection by default" (Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita) di cui all'Articolo 25 del RGPD: p. 1, paragrafo 4.

[403] I "sette principi fondanti" sono: 1. Proattivo e non reattivo, preventivo e non correttivo; 2. Tutela della vita privata come impostazione predefinita; Tutela della vita privata radicata nella progettazione; 4. Piena funzionalità — A somma positiva e non a somma zero; 5. Sicurezza end-to-end — Protezione del ciclo di vita completo; 6. Visibilità e trasparenza — Niente segreti; 7. Rispetto della privacy dell'utente — Misure incentrate sull'utente [nota originale]. Si veda: https://www.ipc.on.ca/wp-content/uploads/2018/01/pbd.pdf.

[404] Per i dettagli su questi elementi nell'interpretazione del GEPD, si veda il Parere preliminare 5/2018 (nota 402, *supra*), pp. 6 – 7 (paragrafi 27 – 32).

Il testo, inoltre, aggiunge:[405]

> **Tutte le quattro dimensioni hanno pari importanza, sono parte integrante dell'obbligo di responsabilizzazione** e saranno sottoposte al controllo delle Autorità di protezione dati, laddove opportuno.

Il GEPD sottolinea l'importanza della protezione dei dati fin dalla progettazione e della protezione per impostazione predefinita per tutta una serie di attori: titolari e responsabili in generale;[406] sviluppatori di prodotti e tecnologie (con impatto privacy);[407] servizi di comunicazione elettronica;[408] servizi di identità elettronica;[409] fornitori di contatori e reti intelligenti.[410] Per quanto riguarda le **amministrazioni pubbliche**, il GEPD rileva che:[411]

> L'Articolo 25 si applica a tutti i tipi di organizzazione che fungono da titolari, comprese le **amministrazioni pubbliche** che, per il loro ruolo a servizio del bene pubblico, **dovrebbero dare l'esempio proteggendo i diritti e le libertà individuali delle persone.** Il RGPD sottolinea il ruolo della protezione dei dati dalla progettazione e della protezione per impostazione predefinita nell'identificazione di fornitori di prodotti e di servizi da parte delle amministrazioni pubbliche al Considerando 78, in base al quale ***"i principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici"*. Le amministrazioni pubbliche sono chiamate ad essere in prima fila nell'applicazione di tali principi in maniera responsabile, pronte a dimostrare la loro attuazione, se necessario, alle competenti Autorità di controllo.**

Il riferimento agli ***appalti pubblici*** riveste un'importanza particolare: i RPD devono ***informare*** le rispettive organizzazioni che, nell'indire tali gare, le amministrazioni pubbliche dovrebbero espressamente ricercare candidati in grado di "dimostrare" che i loro prodotti o servizi sono in tutto conformi al RGPD (e alle legislazioni nazionali e unionali in materia di protezione dei dati personali),[412] e che la protezione dei dati fin dalla progettazione e la protezione per impostazione predefinita sono integrate nei loro prodotti o servizi. Sarebbe, inoltre, opportuno conferire a questi candidati un ***vantaggio competitivo*** rispetto a coloro che offrono prodotti o servizi che non risultano conformi a queste prescrizioni.[413]

Il GEPD analizza in modo approfondito le diverse **metodologie** che sono state sviluppate per implementare la protezione dei dati " by design" e "by default".[414] Non possiamo trattarne in questa sede, ma i RPD dovrebbero averne una conoscenza approfondita (anche oltre i dettagli

---

405 *Idem*, p. 7, paragrafo 32, sottolineatura in grassetto aggiunta.

406 *Idem*, p. 7, paragrafi 35 – 36.

407 *Idem*, p. 7, paragrafo 37.

408 *Idem*, pp. 8 – 9, paragrafi 42 – 44 (con riferimento alla Direttiva e-Privacy e alla proposta di Regolamento e-Privacy).

409 *Idem*, p. 9, paragrafo 45 (con riferimento al Regolamento eIDAS).

410 *Idem*, pp. 9 – 10, paragrafi 46 – 50 (con riferimento alla Raccomandazione sulla scheda di valutazione d'impatto - DPIA dei contatori intelligenti).

411 *Idem*, p. 8, paragrafo 38, originale in corsivo, sottolineatura in grassetto aggiunta.

412 Si veda la discussione sul principio di "responsabilizzazione" nella Seconda Parte, sezione 2.4, *supra*.

413 Questa impostazione è stata apertamente recepita dalla legislazione sulla protezione dei dati dello Schleswig-Holstein.

414 GEPD, Parere preliminare 5/2018 (nota 402, *supra*), pp. 13 – 15, paragrafi 63 – 72. Si vedano anche i riferimenti specifici al Programma sulla Privacy Engineering NIST USA, la Relazione sulla Privacy Engineering e la gestione del rischio per i Sistemi federali USA (p. 11, paragrafo 56, note 76 e 74) e l'analisi dell'ENISA del 2014 con un'analisi completa dello stato dell'arte (dell'epoca), (p. 12, paragrafo 59, nota 82).

del documento del GEPD). Sia sufficiente sottolineare che il **GEPD, a giusto titolo, evidenzia il rapporto fra la protezione dei dati fin dalla progettazione e la protezione per impostazione predefinita e la DPIA (valutazione d'impatto sulla protezione dei dati),** di cui al Compito 4, *supra*;[415] e più in generale rileva esplicitamente che:[416]

> **Il ruolo dei responsabili della protezione dei dati e della privacy è fondamentale ed il loro coinvolgimento è cruciale in un approccio orientato alla "privacy by design".** Devono far parte del processo fin dalle prime fasi, quando le organizzazioni pianificano i sistemi di trattamento dei dati personali, al fine di sostenere, qualora necessario, le dirigenze, i responsabili di settore o attività, e i servizi informatici e tecnologici. Le loro competenze devono corrispondere a questi bisogni.

Questo "insieme di competenze" include l'essere **pienamente formati ed istruiti nelle metodologie e nelle tecnologie da applicare** (se necessario, con un'ulteriore formazione sul campo) **nonché un ampio ed esteso coinvolgimento nella progettazione, nello sviluppo, nel collaudo e nella messa a punto di tutti i prodotti, i servizi e le iniziative della propria organizzazione** (appalti compresi, come abbiamo visto) **che abbiano impatti in termini di privacy.**

- o – O – o –

415 *Idem*, p. 8, paragrafi 39 – 40.

416 *Idem*, p. 15, paragrafo 76, corsivo aggiunto.

COMPITO 10. Consulenza e monitoraggio della conformità delle politiche di protezione dei dati, dei contratti di contitolarità, titolare-titolare e titolare-responsabile, norme vincolanti di impresa e clausole per il trasferimento dei dati.

Per conformarsi ai requisiti del RGPD, e soprattutto per poter "dimostrare" tale conformità, i titolari devono adottare o sottoscrivere tutta una serie di misure. Come rilevato alla sezione 2.2, *supra*, tali misure comprendono:

- la definizione e l'adozione formale di **politiche** interne adeguate in materia **di protezione dei dati** (si veda l'Art. 24(2)) riguardanti:
  - ✓ i **moduli cartacei**, **elettronici e le informative sulla protezione dei dati /privacy pubblicate sui siti web** dell'organizzazione, l'utilizzo di **cookie** e di altri strumenti di monitoraggio;
  - ✓ **log di accesso e di alterazione**, ecc. in software e hardware;
  - ✓ il rilascio di "**patch**" per il proprio software;
  - ✓ eccetera;
- l'adozione di **accordi amministrativi** ("**accordi**") fra autorità o enti pubblici, soprattutto se considerati "**contitolari**" per determinati trattamenti;
- l'elaborazione e la stipula di **contratti con altri titolari e responsabili**; e
- la stesura di o l'adesione a **contratti (standard o autorizzati singolarmente) per il trasferimento dei dati**.

Il principale elemento che merita di essere qui ribadito è che tutte queste sono soprattutto responsabilità ("dimostrazione della conformità" significa questo) del titolare e non tanto del RPD (si veda il punto sulla "*Non responsabilità del RPD nella conformazione ai requisiti del RGPD*", Seconda Parte, sezione 2.5.4, *supra*).

Tuttavia, ancora una volta, nella pratica, il RPD deve essere attivamente coinvolto. Ogni nuovo RPD – e soprattutto quello nominato da un'organizzazione che ne era precedentemente sprovvista – deve poter almeno **revisionare** ogni documento e procedura esistente in materia di protezione dei dati personali per verificarne la piena conformità ai requisiti di legge.

Sulla base di questa revisione, il RPD ha facoltà di **raccomandare modifiche alla documentazione esistente, ecc.** – soprattutto se redatta ed adottata prima dell'entrata in vigore del RGPD – e di **raccomandare l'elaborazione e l'adozione di nuovi documenti** a suo parere necessari, ma inesistenti.

Il RPD è formalmente incaricato di **controllare** la conformità con politiche, accordi o contratti adottati o stipulati dal titolare in relazione al trattamento dei dati personali (cfr. Art. 39(1)(b)).

COMPITO 11. Coinvolgimento nei codici di condotta e nelle certificazioni.

Abbiamo rilevato nella Seconda parte, sezione 2.2, *supra*, che l'adesione e la piena conformità alle norme che figurano in un **codice di condotta** riconosciuto o ad una **certificazione sulla protezione dei dati**, anch'essa riconosciuta, possono costituire un elemento o uno strumento importante per dimostrare la conformità al RGPD in rapporto alle materie oggetto di quel codice o di quella certificazione (anche se non configurano una presunzione di conformità in termini giuridici).

Ancora una volta, è compito del titolare – e non del RPD – decidere se sottoscrivere un codice pertinente al settore in cui opera l'organizzazione, o cercare di ottenere una certificazione della protezione dei dati del tipo previsto dal Regolamento (Articoli 40 – 43). Sarebbe, comunque, del tutto legittimo che un RPD **raccomandasse** un'azione in tal senso.

Inoltre, sarebbe anche auspicabile che i RPD di organizzazioni che operano in un determinato settore partecipassero alla stesura di **(un) codice (i) di condotta** per quel settore, un esercizio destinato a coinvolgere anche altri attori (consulenti legali, personale dell'organismo di settore sotto la cui egida viene redatto il singolo codice - in particolare, personale specializzato in tecnologie dell'informazione e della comunicazione, qualora il codice disciplinasse materie tecniche quali sicurezza ICT, crittografia, …).

Il RPD può anche **coadiuvare l'ottenimento di una certificazione** da parte della sua organizzazione, raccogliendo o fornendo, all'Ente di certificazione in questione, "ogni informazione ed accesso alle attività di trattamento necessarie a espletare la procedura di certificazione" (Art. 42(6)). Tuttavia, qualora uno schema di certificazione si basi sulla **valutazione** delle attività di trattamento del titolare operata da uno o più ***esperti indipendenti*** accreditati da un competente Ente di certificazione (come previsto per esempio dallo schema di certificazione *European Privacy Seal [EuroPriSe]*),[417] il RPD non può intervenire perché ciò configurerebbe un conflitto di interessi.

Nota: la documentazione dettagliata delle valutazioni di impatto (DPIA), di cui abbiamo parlato al Compito 4, e il monitoraggio dei trattamenti su base continuativa di cui al Compito 5 (unitamente alla documentazione di tale attività di monitoraggio), assolvono in certa misura a una funzione simile a quella delle certificazioni perché tale documentazione dimostra che il titolare ed i suoi collaboratori hanno attentamente preso in esame tutte le implicazioni relative alla privacy/protezione dei dati delle specifiche attività di trattamento, adottando le opportune misure correttive. Il vantaggio delle certificazioni consiste nel fatto che le valutazioni sono compiute da esperti indipendenti esterni. Molto dipende, comunque, dalla qualità degli schemi riconosciuti di certificazione e dalle interazioni fra tali schemi e le attività di enforcement delle singole Autorità di controllo.

- o – O – o -

[417] Si veda: https://www.european-privacy-seal.eu/EPS-en/fact-sheet

Cooperazione e consultazione con l'autorità di protezione dati

COMPITO 12. Cooperazione con l'autorità di protezione dati.

Il RPD ha il compito di rispondere alla richieste della DPA e, nella sfera delle proprie competenze, collaborare con l'Autorità di controllo su sua richiesta o su propria iniziativa. (Art. 39(1)(d)).

A questo proposito il WP29 afferma che:[418]

> Questi compiti attengono al ruolo di "facilitatore" attribuito al RPD e già menzionato nell'introduzione alle presenti linee guida. Il RPD funge da punto di contatto per facilitare l'accesso, da parte dell'autorità di controllo, ai documenti e alle informazioni necessarie per l'adempimento dei compiti a lei attribuiti dall'articolo 57 nonché ai fini dell'esercizio dei poteri di indagine correttivi, autorizzativi e consultivi di cui all'articolo 58. Si è già rilevato che il RPD è tenuto al rispetto delle norme in materia di segreto o riservatezza, in conformità al diritto dell'Unione o degli Stati membri (Articolo 38(5)). Tuttavia, tali vincoli di segreto/riservatezza non precludono la possibilità per il RPD di contattare e chiedere lumi all'autorità di controllo. L'Articolo 39(1)(e) prevede che il RPD possa consultare l'autorità di controllo con riguardo a qualsiasi altra questione, se del caso.

Il GEPD ha trattato approfonditamente i compiti equivalenti dei RPD delle istituzioni dell'UE nella loro relazione con il GEDP, come si può chiaramente rilevare nelle citazioni che seguono. I testi sono stati emendati per applicarli , *mutatis mutandis*, alla relazione fra le Autorità di protezione dei dati degli Stati membri (DPA) (e il GEPD) e i RPD nominati ai sensi del RGPD. Prima di tutto viene fatto notare, in termini generali, che:[419]

> Il RPD ha il compito di rispondere alle richieste della [DPA di riferimento] e, nel proprio ambito di competenza, di cooperare con la [DPA] su richiesta di quest'ultima o per iniziativa propria. Questo compito mette in evidenza il fatto che il RPD facilita la cooperazione fra la [DPA] e l'istituzione, soprattutto nel caso di indagini, di trattamento dei reclami e di verifiche preliminari. Il RPD non solo conosce il funzionamento interno dell'istituzione, ma conoscerà probabilmente anche la persona migliore da contattare al suo interno. Il RPD può essere anche a conoscenza e informare la [DPA] dei recenti sviluppi suscettibili di avere un impatto sulla protezione dei dati personali.

Il GEPD affronta, a tal proposito, una serie di punti che, nella loro formulazione, trovano applicazione anche alle analoghe attività connesse al RGPD:[420]

> **IV. Relazione RPD – [DPA]**
>
> Il rispetto del regolamento dipenderà dalla relazione di lavoro fra il RPD e la [DPA di riferimento]. Il RPD non deve essere considerato un agente della [DPA], ma un esperto facente parte dell'istituzione/organismo in seno al quale o per il quale lavora. Come già menzionato, l'idea di prossimità lo mette in una posizione ideale per vigilare, dall'interno, alla conformità al regolamento e formulare consigli o intervenire tempestivamente evitando così un eventuale intervento dell'autorità di controllo. Allo stesso tempo, la [DPA] può offrire un sostegno prezioso al RPD nell'esercizio delle sue

418 Linee guida sui RPD del WP 29, p. 18.
419 GEPD, Documento di sintesi sui RPD, p. 6. Modifiche rispetto al testo in parentesi quadre.
420 *Idem*, Parte IV (pp. 10 – 11).

funzioni. [421] La [DPA è di conseguenza][422] favorevole all'idea di sviluppare possibili sinergie fra i RPD e le [DPA] per la realizzazione dell'obiettivo globale di una protezione efficace dei dati personali in seno alle istituzioni ….

IV. 1. Garantire il rispetto del regolamento.

Per garantire il rispetto del regolamento bisogna cominciare soprattutto dalla sensibilizzazione. Come detto, i RPD giocano un ruolo importante nello sviluppo delle conoscenze in materia di protezione dei dati in seno alla loro istituzione/organismo. Le [DPA accolgono][423] favorevolmente questo ruolo ed il fatto che possa favorire un approccio preventivo efficace, piuttosto che un controllo repressivo della protezione dei dati.

Il RPD fornisce, inoltre, all'istituzione/organismo consigli pratici finalizzati al miglioramento della protezione dei dati in seno all'istituzione/organismo stesso o all'interpretazione o all'applicazione del [RGPD].[424] Questa funzione è condivisa con le [DPA] che consigliano tutte le istituzioni o istanze [nazionali] sulle questioni inerenti il trattamento dei dati personali ([Articolo 57(1)(c) RGPD])). In questo campo, le [DPA nazionali sono spesso già state invitate nel passato] ad offrire consigli ai RPD su problemi specifici inerenti la protezione dei dati (approccio caso per caso). Le [DPA e il GEPD potranno verosimilmente] redigere dei documenti di sintesi (position paper) su temi specifici per offrire orientamenti alle istituzioni/organismi su argomenti più generali.[425]

IV.2 Verifiche preliminari

I pareri elaborati [da una DPA] nel quadro dell'[Articolo 36 del RGPD relativo alle consultazioni preliminari] [e i pareri espressi dalle DPA nell'iter delle autorizzazioni preliminari di cui all'articolo 36(5) del RGPD], costituiscono l'occasione per la [DPA] di controllare e garantire la conformità al [RGPD]. …

… [P]rima dell'adozione definitiva di un parere frutto di una verifica preliminare, la [DPA ha facoltà di][426] inviare [] al RPD una versione provvisoria contenente informazioni sulle raccomandazioni previste, il che permette di discuterne l'efficacia e le conseguenze. Le

---

[421] Vedi la messa a disposizione, da parte della CNIL, **l'Autorità francese** della protezione dei dati, di uno speciale "*extranet*" per RPD accreditati, accessibile solo con username e password, che mette on line testi giuridici (leggi, decreti, ecc.), formazioni ed informazioni (fra cui le ultime relazioni e linee guida pubblicate dal CNIL e gli ultimi orientamenti pratici e normativi in materia) offrendo ai RPD una piattaforma di discussione e scambio di punti di vista. V. la sezione 2.3.5 alla voce "Formazione e certificazione".

[422] Il testo originale afferma che il GEPD "sostiene" l'idea. Le DPA (e il Comitato Europeo per la protezione dei dati - EDPB) dovrebbero essere dello stesso parere.

[423] Il testo originale afferma che il GEPD "accoglie con favore" questo approccio, ma (anche alla luce delle prassi del passato) le DPA (e l'EDPB) dovrebbero comunque essere dello stesso parere.

[424] Il documento del GEPD fa riferimento al Regolamento che stabilisce le norme sulla protezione dei dati per le Istituzioni dell'UE (Regolamento (CE) 45/2001), ma lo stesso vale in relazione al RGPD per i RPD nominati ai sensi di quest'ultimo Regolamento. Abbiamo operato analoghe sostituzioni anche in altri punti della citazione.

[425] Il testo originale afferma che il GEPD "intende elaborare" documenti di orientamento e pareri scritti. Ancora una volta, le DPA nazionali e l'EDPB dovrebbero fare lo stesso per quanto riguarda il RGPD.
La frase omessa recita: "Per quanto riguarda i RPD nominati ai sensi del RGPD, le DPA nazionali, ma soprattutto il nuovo EDPB, elaboreranno sicuramente orientamenti simili".

[426] La prassi di inviare una "bozza provvisoria di raccomandazione" a un titolare nel contesto di un processo di "verifica preliminare"/"autorizzazione preliminare" non è specificata nel RGPD (o nel Regolamento 45/2001). Che il RGPD faccia comunque riferimento ad una "*consultazione* preliminare" gioca fortemente a favore del fatto che le DPA, a titolo di detto strumento, adotteranno un approccio simile; il dettato della frase (in parentesi quadra), aggiunto due volte a questo paragrafo, lo conferma ulteriormente.

[DPA vogliono essere] attente alle preoccupazioni delle istituzioni, espresse per il tramite del RPD, allo scopo di formulare raccomandazioni realizzabili.

IV. 3. Esecuzione

Per quanto riguarda l'attuazione di misure specifiche di protezione dei dati, esistono sinergie potenziali fra i RPD e le [DPA] sull'adozione di sanzioni e il trattamento dei reclami e delle denunce.

Come già affermato, i RPD hanno poteri limitati di esecuzione. La [DPA] contribuirà a garantire il rispetto del [RGPD] prendendo misure efficaci in materia di [consultazioni o autorizzazioni] preliminari e di trattamento dei reclami e delle denunce. Le misure sono efficaci se ben mirate e realizzabili: il RPD può anche essere considerato un partner strategico per determinare l'applicazione corretta di una misura.

Il trattamento dei reclami e delle richieste da parte del RPD a livello locale [427] deve essere incoraggiato almeno per quanto riguarda la prima fase dell'indagine e la soluzione del problema. Le [DPA dovrebbero][428] quindi [ritenere] che il RPD abbia almeno la possibilità di esaminare e trattare i reclami a livello locale prima di riferirne alla [DPA]. Il RPD dovrebbe, inoltre, … consultare la [DPA] in caso di dubbi sulla procedura o sul contenuto dei reclami. Questo non impedisce, tuttavia, alla persona interessata di indirizzarsi direttamente alla [DPA] ai sensi dell' [Articolo 77(1) del RGPD]. I limitati poteri di esecuzione del RPD implicano anche che, in certi casi, il reclamo o la denuncia debbano essere trasmessi alla [DPA]. La [DPA] garantisce quindi un sostegno prezioso in caso di esecuzione. Il RPD, a sua volta, fornisce informazioni alla [DPA] e assicura il follow-up delle misure adottate.

IV.4. Misura dell'efficacia delle disposizioni adottate[429]

Per quanto riguarda l'efficacia delle misure adottate in materia di protezione dei dati, il RPD deve essere considerato un utile alleato per valutarne i progressi. Per esempio, se si tratta di misurare l'efficacia del controllo interno della protezione dei dati, le [DPA incoraggiano] i [] RPD a elaborare criteri propri di controllo della qualità (norme professionali, piani specifici per l'istituzione, programma annuo di lavoro …). Questi criteri permetteranno alla [DPA], quando è invitata a farlo, di valutare il lavoro del RPD, ma anche di misurare lo stato di attuazione del [RGPD] in seno all'istituzione/organismo.

Inoltre, è probabile che i RPD operanti nel settore pubblico siano chiamati dalle competenti Autorità di controllo a contribuire a consultazioni pubbliche lanciate dalle Autorità stesse, e a fornire input nel corso della preparazione da parte dell'Autorità di pareri formali su

---

427 Rileviamo che la gestione delle domande e dei reclami dei soggetti interessati viene ulteriormente discussa al Compito 11, *infra*.

428 Le prime due frasi del paragrafo fanno ancora una volta riferimento alla prassi seguita dal GEPD; comunque, anche alla luce delle esperienze passate, è del tutto probabile che le DPA nazionali seguano la stessa impostazione (come indicato dal dettato nelle parentesi quadre).

429 Non esistono norme specifiche, né nel Regolamento 45/2001 (per quanto riguarda le Istituzioni dell'UE), né nel RGPD (per quanto riguarda le entità soggette a questo strumento normativo) che diano alle competenti autorità (rispettivamente il GEPD e le DPA nazionali) la possibilità di "misurare l'efficacia" delle misure adottate dai titolari allo scopo di assicurare la conformità alla norma di applicazione. Nel quadro istituzionale dell'UE, il GEPD considera (a giusto titolo) che questo compito faccia naturalmente parte delle sue funzioni. È probabile che le DPA degli Stati membri (e l'EDPB) "incoraggeranno" i RPD a un elevato livello di rispetto delle norme con l'adozione o l'adesione a "standard professionali, piani specifici per istituzione, programmi di lavoro annuali", ecc.; il dettato delle frasi (nelle parentesi quadre) ancora una volta conferma questa interpretazione.

progetti o disegni di legge in materia di protezione dati che incidano sugli ambiti di attività degli stessi RPD.

Va rilevato, infine, che il RPD ha un ruolo importante nel coadiuvare la DPA ad effettuare ispezioni in loco, consultazioni con i titolari in settori specifici, ecc. È raro, ad esempio, che le DPA effettuino controlli senza preavviso – un caso di specie si può solo verificare qualora i sospettati possano nascondere dati o prove se messi al corrente di un'indagine in corso. Nella pratica, le DPA di solito concordano le ispezioni con l'aiuto del titolare, e in particolare del RPD del titolare, che garantisce la disponibilità delle persone interessate e delle aree e dei sistemi che devono essere oggetto del controllo. Si tratta di un aiuto fondamentale, soprattutto se parliamo di sistemi di trattamento complessi e che richiedono conoscenze approfondite delle architetture ICT e dei processi interni per essere adeguatamente valutati. Quando una DPA vuole esaminare nel dettaglio il trattamento dei dati personali in un determinato contesto o settore – fissando, come fanno la maggior parte delle Autorità, un piano di lavoro annuo e selezionando le loro priorità – chiede al RPD del titolare che opera in quel contesto o in quel settore quale è la situazione, organizza riunioni con le parti interessate e procede a consultazioni. Anche questo fa parte integrante di quello che il GEPD chiama il "partenariato strategico" fra i RPD e le DPA.

- o – O – o -

Gestione delle richieste dell'interessato

COMPITO 13. Gestione di richieste e reclami dell'interessato

Il RGPD stabilisce che:

> 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.
>
> (Art. 38(4))

Gli **interessati** che vogliono esercitare i loro **diritti** – diritto di accesso, di rettifica e cancellazione ("diritto all'oblio"), limitazione di trattamento, portabilità dei dati, diritto di opposizione in generale e in relazione a processi decisionali automatizzati e alla profilazione – o che hanno **domande generali** o **reclami** in materia di protezione dei dati da presentare nei confronti di un determinato soggetto o organismo, o ente, generalmente dovranno per prima cosa indirizzarsi al RPD (se ne è stato nominato uno).

La procedura è facilitata dal fatto che il RGPD prevede che i recapiti del RPD siano pubblicati dall'organizzazione (Art. 37(7)) e che il titolare del trattamento si assicuri "*che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali [relativi all'organizzazione]*" (Art. 38(1)). Di conseguenza, se l'interessato si rivolge a qualcun altro nell'organizzazione, pensiamo all'Amministratore delegato o a un consigliere generale, costui dovrebbe trasmettere la richiesta al RPD.

Inoltre, lo statuto indipendente del RPD (Art. 38(3)) garantisce che la richiesta, il reclamo o la denuncia siano gestiti dal RPD – o dal personale responsabile sotto la supervisione del RPD – in **modo appropriato, senza favoritismi per l'organizzazione o discriminazioni per l'interessato.** Il RPD ha comunque il compito di scrivere, o riesaminare, la risposta all'interessato facendo presente che, nel caso in cui non sia soddisfatto, egli ha sempre facoltà di presentare il caso alla DPA.

Infatti, in ogni caso, è diritto dell'interessato presentare richieste, reclami e denunce all'organizzazione (ossia, al RPD dell'organizzazione) **fermo restando il diritto di ricorrere alla DPA**. Nello specifico, ciascuna DPA ha il dovere e i poteri, nella propria giurisdizione, di:

> trattare i reclami proposti da un interessato …, svolgere le indagini opportune sull'oggetto del reclamo e informare il reclamante dello stato e dell'esito delle indagini.
>
> (Art. 57(1)(f)).

Nel reclamo alla DPA, l'interessato può farsi rappresentare da un organismo senza scopo di lucro (Art. 80); i doveri ed i poteri della DPA relativi alla trattazione di questi reclami (vedi *supra*) sono estesi anche a questi casi (si veda il dettato di cui all'Articolo 57(1)(f), omesso dalla precedente citazione).

In tal senso, i RPD potrebbero anche dare risposta alle richieste e ai **reclami di queste organizzazioni rappresentative**, e non soltanto a quelle dei soggetti interessati.

Come abbiamo notato parlando del Compito 10 (*Cooperazione con la DPA)*, è prevedibile (anche alla luce delle passate prassi) che le DPA nazionali (come il GEPD in relazione ai RPD delle Istituzioni dell'UE) incoraggino gli interessati (e le organizzazioni rappresentative suddette) a interpellare in prima battuta direttamente il titolare e, nello specifico, il RPD del

titolare, rispetto a eventuali problematiche così verificare se possano essere esaminate e risolte già a questo livello e in modo soddisfacente, senza quindi coinvolgere la DPA, fermo restando che il RPD ha sempre il dovere di consultare la DPA su problemi di interpretazione generale e di applicazione del RGPD. Questo approccio, comunque, non deve mai scoraggiare gli interessati (o le organizzazioni rappresentative di interessi diffusi) dall'affrontare questioni – soprattutto di principio – con la DPA.

Come afferma il GEPD, l'Autorità di controllo e i RPD danno vita ad un "partenariato strategico": le DPA incoraggiano gli interessati (in primo luogo e soprattutto) a risolvere eventuali problemi direttamente con i RPD; i RPD devono essere in grado – ed hanno il compito – di collaborare con l'Autorità per garantire che le risposte alle domande e ai reclami siano gestite in modo corretto e producano, se del caso, i cambiamenti necessari nelle prassi del titolare. Le DPA devono poter fare affidamento sui RPD e sulla loro capacità di essere al fianco degli interessati per qualsiasi reclamo e i RPD devono poter contare sulle DPA affinché sia data effettiva esecuzione alle proposte di cambiamento.

Per questo la posizione del RPD, di cui abbiamo parlato nella Seconda Parte, sezione 2.5, è così delicata: i RPD sono dei "ponti" fra il titolare e l'Autorità e non dovrebbero ritrovarsi fra l'incudine e il martello.

- 0 – O – o -

Informazione e sensibilizzazione

COMPITO 14. Compiti di informazione e di sensibilizzazione interna ed esterna.

Il RGPD precisa che il RPD è incaricato "almeno di":

> 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.
>
> (Art. 39(1)(a))

Internamente, (cioè nell'organizzazione in cui il RPD lavora), questo implica, da un lato, che il RPD **informi** i membri del personale dei loro diritti e, dall'altro lato, che **istruisca** i titolari, le organizzazioni e i membri del personale – inclusi, in particolare, i "responsabili di settore"/i responsabili di operazioni specifiche – su obblighi e responsabilità e li **formi** al loro rispetto.

Come afferma il GEPD in un testo citato precedentemente:[430]

> Per garantire il rispetto del regolamento bisogna cominciare soprattutto dalla sensibilizzazione … i RPD giocano un ruolo importante nello sviluppo delle conoscenze in materia di protezione dei dati in seno alla loro istituzione/organismo.

La sensibilizzazione "permette un approccio preventivo efficace piuttosto che un controllo repressivo della protezione dei dati.".[431]

Le misure adottate dal RPD a tal fine includono l'elaborazione di **note (o circolari) di informazione al personale**, l'organizzazione di sessioni interne di formazione sulla protezione dei dati – finalizzate a sensibilizzare e migliorare la consapevolezza sulla protezione dei dati e i diritti dei soggetti interessati, cioè alla creazione di un "riflesso automatico" di protezione dei dati a tutti i livelli della vita sociale, in quanto semplici cittadini, lavoratori, team leader, dirigenti.

In queste misure includiamo anche la creazione di un **sito web** interno di informazione e didattica sulla protezione dei dati e la redazione e l'invio di **informative sulla privacy** sui siti web e le pagine web del personale.[432]

All'esterno, oltre a garantire che agli interessati siano fornite tutte le informazioni necessarie al momento della prima raccolta dei dati che li riguardano (come stabilito agli Articoli 12 – 14 del RGPD), ad es. attraverso comunicazioni redatte con chiarezza nei siti web, il RPD deve collaborare con il personale delle relazioni pubbliche per garantire la **piena trasparenza sulle attività di trattamento dei dati personali dell'organizzazione**, sulle finalità di raccolta e sul trattamento dei dati personali, sulle categorie dei soggetti dei dati e dei dati interessati, sui destinatari dei dati, sull'eventuale trasferimento dei dati a Paesi terzi (non-UE/SEE); ecc.

Il RGPD non impone ai titolari di rendere di dominio pubblico il registro delle attività di trattamento dei dati personali, [433] anche se certamente non lo vieta.

---

430 GEPD, Documento di sintesi sui RPD (nota 240, *supra*), p. 10.

431 *Idem*.

432 *Idem*, p. 5.

433 La Direttiva sulla protezione dei dati del 1995 obbligava le DPA a rendere di pubblico dominio i dettagli delle operazioni di trattamento loro notificate (Art. 21).

Il GEPD è fortemente a favore della pubblicazione per le Istituzioni dell'UE, in quanto (come previsto dalla Direttiva sulla protezione dei dati del 1995) un precedente regolamento le obbligava alla pubblicazione dei dettagli della notifica "equivalenti in termini funzionali":[434]

> I registri sono uno strumento importante per controllare e documentare che l'organizzazione abbia il controllo delle attività di trattamento … .
>
> **Il GEPD raccomanda fortemente che le [Istituzioni dell'UE] rendano i registri accessibili al pubblico, preferibilmente tramite pubblicazione in internet … .**
>
> I registri dovrebbero essere pubblici in quanto ciò:
>
> - contribuisce alla trasparenza degli IUE;
> - rafforza la fiducia dell'opinione pubblica;
> - facilita la condivisione delle conoscenze fra IUE;
> - e il non farlo sarebbe un passo indietro e un ritorno alle [regole] del passato.

Lo stesso si può dire per il registro delle attività di trattamento che deve essere tenuto dai titolari ai sensi del RGPD – quanto meno per quanto riguarda le autorità pubbliche. Alcuni Stati membri impongono nel diritto nazionale l'obbligo di pubblicazione dei dettagli del registro, ma le autorità pubbliche dei paesi in cui questo obbligo non è ancora in vigore possono sempre farlo alla luce delle osservazioni del GEPD.

Titolari e responsabili del trattamento, naturalmente, non hanno l'obbligo di pubblicare informazioni sui meccanismi di sicurezza che potrebbero essere utilizzate per commettere violazioni della sicurezza (come già riconosciuto dalle disposizioni della Direttiva sulla protezione dei dati del 1995 in materia di pubblicazione dei dettagli dei trattamenti notificati alle DPA).[435]

Le informazioni di base sui trattamenti di dati personali effettuati dall'organizzazione dovrebbero comunque essere di facile accesso **sul sito web** dell'organizzazione stessa ed essere presenti anche in **pieghevoli** e **formulari** (comprese le versioni destinate alle persone disabili).

I siti web e i formulari dovrebbero anche dettagliare **come gli interessati possano esercitare i loro diritti** (con una chiara comunicazione dei **contatti del RPD** – anche senza menzionarne cognome e nome); quali **codici di condotta** siano stati sottoscritti dall'organizzazione, quali **certificazioni** siano state ottenute (attraverso **loghi o sigilli** riconosciuti), ecc.

Ogni sito web, naturalmente, dovrebbe rispettare tutte le norme Ue in materia di protezione dei dati oltre alle legislazioni nazionali in materia, per quanto riguarda i **cookie** e altri strumenti di monitoraggio, ecc.

- o – O – o -

---

434 GEPD, Responsabilizzazione dei soggetti locali (Accountability on the ground), p. 8, in corsivo nell'originale.

435 Si veda nuovamente l'Articolo 21 della Direttiva sulla protezione dei dati del 1995 che esclude le informazioni che figurano nella lista di cui all'Articolo 19(1)(f) – vale a dire, una descrizione generale delle misure di sicurezza poste in atto dal titolare – dalle informazioni di dominio pubblico. Si osservi, comunque, che la fiducia nell'approccio denominato "sicurezza tramite oscuramento" ha perso da tempo credibilità. Si veda: https://en.wikipedia.org/wiki/Security_through_obscurity

COMPITO 15. Pianificazione e riesame delle attività del RPD

Infine, tenuto conto della numerosità e dell'ampiezza dei compiti affidati al RPD, è opportuno che l'RPD rediga una pianificazione annuale delle attività alla luce della tempistica necessaria per lo svolgimento di ciascuno di tali compiti e per la gestione di nuovi sviluppi, con un margine di flessibilità in caso di eventuali imprevisti. Egualmente opportuni sono la revisione e l'aggiornamento periodici di tale pianificazione.

Douwe Korff & Marie Georges - Cambridge/Parigi, dicembre 2018/luglio 2019