CONSULENZA
L'informazione integrata per professionisti e aziende

GUIDA RAGIONATA ALL'APPLICAZIONE DEL GDPR

Regolamento (UE) 2016/679 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)

di Nicholas Botti

Buffetti

GUIDA RAGIONATA ALL'APPLICAZIONE DEL GDPR

di Nicholas Botti

SOMMARIO

INTRODUZIONE

Come noto, in data 4 Maggio 2016 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione europea il 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, comunemente detto **GDPR** (***General Data Protection Regulation***). Il Regolamento è entrato in vigore il 25 Maggio 2016, ma si applicherà solamente a decorrere dal 25 Maggio 2018. Il Regolamento ha visto la luce dopo un iter di approvazione lungo e travagliato durato quattro anni e nasce dall'esigenza di affrontare la continua evoluzione del concetto di privacy e protezione dei dati personali, dovuta anche e soprattutto alla sempre maggior diffusione del progresso tecnologico.

Si badi che la scelta dello strumento legislativo regolamentare non è stata casuale: mentre infatti le Direttive prevedono l'adeguamento di ciascuna legislazione nazionale per conformarsi ai requisiti previsti dalla specifica Direttiva, i Regolamenti hanno valore di legge in tutta l'Unione Europea senza la necessità di adeguamento delle legislazioni nazionali. Il Regolamento ambisce ad **armonizzare e rafforzare in una singola legge le differenti leggi** e relative implementazioni che hanno permesso di ottenere livelli di protezione dei dati diversi da Paese a Paese nella stessa Unione Europea.

La tecnologia attuale consente alle imprese (ma anche alle autorità pubbliche) di utilizzare – nello svolgimento delle loro attività – dati personali come mai in precedenza e sempre più spesso sono gli stessi privati a pubblicare in rete le informazioni personali che li riguardano. Conseguentemente, il quadro giuridico attuale, pur rimanendo valido in termini di obiettivi e principi, non ha impedito la frammentazione delle modalità di applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica e la diffusione percezione nel pubblico che le operazioni on line comportino notevoli rischi. Si è reso pertanto necessario predisporre **un quadro giuridico più solido e coerente** in materia di protezione dei dati dell'Unione che, affiancato da efficaci misure di attuazione, consentirà – o perlomeno è quello che ci si auspica – lo sviluppo dell'economia digitale nel mercato interno, garantirà alle persone fisiche il controllo dei loro dati personali e rafforzerà la certezza giuridica e operativa per i soggetti economici e le autorità pubbliche.

1.OBIETTIVI E FINALITÀ DEL GDPR

La protezione delle persone fisiche con specifico riferimento al trattamento dei dati personali è un diritto fondamentale di ciascun individuo, a prescindere dalla nazionalità o dalla residenza. È lo stesso diritto dell'Unione europea a sancirlo con fermezza, tanto nell'art. 8 parag. 1 della Carta dei diritti fondamentali, quanto nell'art. 16 parag. 1 TFUE; entrambe le fonti, infatti, stabiliscono che «ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano».

Il nuovo regolamento, come si evince tra l'altro dal Considerando 2, ha il dichiarato obiettivo di contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alle convergenze delle economie del mercato interno e al benessere delle persone fisiche. Non si può certo non considerare che proprio l'integrazione economica e sociale conseguente al funzionamento del mercato interno ha condotto a un considerevole aumento dei flussi transfrontalieri di dati personali. Non solo, la logica conseguenza è anche un aumento dei dati personali scambiati, in tutta l'Unione (ma non solo), tra attori pubblici e privati, comprese persone fisiche, associazioni e imprese. Questo incessante – e alle volte non propriamente trasparente – scambio di dati può essere portatore di storture e abusi. Il legislatore europeo manifesta in maniera chiara quella che dovrebbe essere la finalità primaria del trattamento dei dati personali: servire l'uomo. Il diritto alla protezione dei propri dati personali, prosegue il legislatore europeo nel Considerando 4, «non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemplato con altri diritti fondamentali».

Lo scambio di dati – la cui portata è aumentata in modo significativo a causa della rapidità dell'evoluzione tecnologica e della globalizzazione – comporta nuove sfide per la protezione dei dati personali. L'attuale tecnologia consente sia alle imprese private che alle autorità pubbliche di utilizzare dati personali in quantità mai raggiunte in precedenza; sempre più spesso, infatti, le persone rendono disponibili al pubblico – e su scala mondiale – informazioni personali che le riguardano.

È di tutta evidenza come la tecnologia abbia trasformato l'economia e le relazioni sociali – se in meglio o in peggio rimane giudizio personale – e la diretta conseguenza dovrebbe essere una facilitazione alla libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali. Non solo, le nuove tecnologie dovrebbero garantire un elevato livello di protezione di tutti i dati scambiati.

È da una tale evoluzione che prende le mosse il Regolamento (UE) 2016/679: è sempre più necessario, date le evoluzioni appena narrate, un quadro solido e coerente in materia di protezione dei dati ed è fondamentale che vengano previste misure efficaci di attuazione. Così facendo si potrà creare quel clima di fiducia necessario a consentire lo sviluppo dell'economia digitale in tutto il mercato interno. Per assicurare un livello coerente di protezione – che si ribadisce ancora una volta deve prescindere dalla nazionalità o dal luogo di residenza – delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, è stato stilato il Regolamento (UE) 2016/679 il quale, oltre a garantire la certezza del diritto e la trasparenza degli operatori economici (comprese le micro, piccole

e medie imprese), offre altresì alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei titolari e dei responsabili del trattamento dei dati personali e, non da ultimo, prevede sanzioni equivalenti in tutti gli Stati membri e assicura una sospensione efficace tra le diverse autorità di controllo statali. Il legislatore europeo suggerisce l'opportunità – che ha però tutta l'aria di essere una necessità – che le persone abbiano il pieno controllo dei dati personali che le riguardano e che la certezza giuridica e operativa sia rafforzata tanto nel loro confronti quanto per gli operatori economici e le autorità pubbliche. Questo si traduce nella previsione di quei diritti degli interessati disciplinati agli artt. 15 e ss. del Regolamento.

I concetti appena espressi vengono sviluppati dal legislatore europeo, ancor prima che nel testo vero e proprio del Regolamento, nei Considerando 9 e 10 che sono certamente parte integrante del dettato normativo ma che ne costituiscono in un certo qual modo, necessaria premessa. Qui il legislatore evidenzia l'odierna permanenza dei principi espressi nella Direttiva 95/46/CE, ma nonostante ciò non si è riuscito a impedire la frammentazione dell'applicazione dei dati personali nel territorio dell'Unione né tantomeno a eliminare l'incertezza giuridica o la percezione – largamente diffusa – che soprattutto le operazioni online comportino rischi per la protezione delle persone fisiche. Pertanto, prosegue il legislatore nel Considerando 10, al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri ed è per questo che è necessario, come sopra enunciato, assicurare un'applicazione omogenea e coerente delle norme poste a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione.

Da ultimo si segnala che è stata pubblicata sulla Gazzetta Ufficiale dell'Unione Europea C192/7 del 30.06.2012 una sintesi del parere del Garante europeo della protezione dei dati del 07.03.2012 sul pacchetto di riforma della protezione dei dati[1].

[1] È possibile visionare il documento al seguente indirizzo http://eur-lex.europa.eu/legal-content/IT/AUTO/?uri=OJ:C:2012:192:TOC

2.AMBITO DI APPLICAZIONE DEL GDPR

2.1 Ambito di applicazione materiale

L'art. 2 definisce in maniera chiara e netta l'ambito di applicazione del Regolamento, specificando quali trattamenti ne sono soggetti e quali invece ne sono sottratti. In primo luogo si applica al trattamento interamente o parzialmente automatizzato di quei dati personali che sono contenuti in un archivio o che sono destinati a figurarvi. Il motivo di una tale apertura risiede nella convinzione del legislatore europeo che la protezione delle persone fisiche – per evitare l'insorgere di gravi rischi di elusione – debba essere il più possibile neutrale sotto il profilo tecnologico e indipendente dalle tecniche impiegate per il trattamento dei dati.

Il regolamento non si applica, invece, ai trattamenti:

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

√ effettuati dagli Stati membri nell'esercizio di attività in materia di politica estera e sicurezza comune;

√ effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico, quindi a quelle attività che sono prive di una connessione con un'attività commerciale o professionale. Tali attività potrebbero comprendere la corrispondenza e gli indirizzari o l'uso dei social network o ancora le attività online intraprese nel quadro di tali attività. Tuttavia, specifica il legislatore nel Considerando 18, il regolamento è pienamente applicabile ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico;

√ effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse. Tali dati sono disciplinati da un più specifico atto dell'Unione, vale a dire la Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio. Gli Stati membri possono però conferire alle autorità competenti altri compiti che non siano necessariamente svolti per le finalità poc'anzi indicate; in tal caso ben potrebbe accadere che il trattamento di dati effettuati in tali diversi ambiti ricada nell'ambito di applicazione del regolamento (UE) 2016/679 rendendovi così soggette anche tali autorità. In quest'ultimo caso è prevista la possibilità per gli Stati membri di mantenere o introdurre disposizioni più specifiche per meglio adattare l'applicazione delle disposizioni del Regolamento. Queste disposizioni potranno determinare con maggiore precisione requisiti specifici per il trattamento di dati personali, tenuto conto della struttura costituzionale, organizzativa e amministrativa dei rispettivi Stati membri.

Per quanto riguarda il trattamento dei dati personali effettuato da istituzioni, organi, uffici e agenzie dell'Unione si applica, per espressa previsione, il Regolamento (CE) n. 45/2001 il quale dovrà essere – così come gli altri atti giuridici dell'Unione applicabili a tale trattamento – adeguato ai principi e alle norme del Regolamento (UE) 2016/679.

All'ultimo paragrafo, l'art. 2 stabilisce che il Regolamento non pregiudica l'applicazione della Direttiva 200/31/CE, la quale contribuisce al buon funzionamento del mercato interno garantendo la libera circolazione dei servizi della società dell'informazione[2] tra Stati membri. In particolare non viene pregiudicata l'applicazione delle norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli artt. 12-15 della Direttiva 2000/31/CE, vale a dire: semplice trasporto ("*mere conduit*"), memorizzazione temporanea ("*coaching*"), *hosting*. L'art. 15 stabilisce, così come si evince dalla sua rubrica, un'assenza sia dell'obbligo generale di sorveglianza sulle informazioni trasmesse o memorizzate dagli Stati membri nella prestazione dei servizi appena elencati, sia di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite[3].

2.2 Ambito di applicazione territoriale

In via generale, l'art. 3 stabilisce che il Regolamento si applichi al trattamento dei dati personali – effettuato da un titolare o da un responsabile del trattamento – che avvenga nell'ambito delle attività di uno stabilimento situato nell'Unione, ciò indipendentemente dal fatto che il trattamento avvenga concretamente all'interno dell'Unione[4]. È del tutto ininfluente la forma giuridica assunta: lo stabilimento implica l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile, la quale può essere anche una succursale a una filiale dotata di personalità giuridica.

Il legislatore, onde evitare che una persona fisica venga privata della protezione cui ha diritto in base al Regolamento, ha previsto ulteriori ipotesi di operatività del Regolamento. Nello specifico, le sue disposizioni si applicano anche al trattamento dei dati personali di soggetti che si trovano all'interno dell'Unione, operato da un titolare o da un responsabile che, al contrario, non siano stabiliti nell'Unione. Ciò avviene, però, unicamente per le seguenti attività:

√ offerta di beni o prestazioni di servizi, indipendentemente dall'obbligatorietà di un pagamento dell'interessato. Per determinare se il titolare o il responsabile del trattamento stiano offrendo beni o servizi all'interessato è opportuno verificare se gli stessi intendono fornire servizi agli interessati in uno o più Stati membri dell'Unione. Il legislatore, nel Considerando 23, fornisce alcune indicazioni utili a individuare una tale intenzione. La semplice accessibilità del sito web del titolare, del responsabile o dell'intermediario

[2] Per "servizi della società dell'informazione" si intende qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizio.
[3] L'art. 15 dispone inoltre che «Gli Stati membri possono stabilire che i prestatori di servizi della società dell'informazione siano tenuti ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati.».
[4] In questo modo il nuovo regolamento rivede la concezione tradizionale del principio di stabilimento del territorio.

dell'Unione, di un indirizzo di posta elettronica o di altre coordinate di contatto o infine l'impiego di una lingua abitualmente utilizzata nel Paese terzi in cui il titolare è stabilito sono, a detta del legislatore, insufficienti ad accertare la suddetta intenzione; al contrario, fattori quali l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni e servizi in tale altra lingua, o ancora la menzione di clienti o utenti che si trovano nell'Unione, possono evidenziare l'intenzione del titolare o del responsabile del trattamento di fornire beni o servizi agli interessati dell'Unione;

√ monitoraggio del comportamento dell'interessato nella misura in cui questo abbia luogo all'interno dell'Unione. Per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone interessate sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali.

Ultima ipotesi di applicazione del regolamento (art. 3 parag. 3) è quella del trattamento dei dati personali effettuato da un titolare che non è stabilito nell'Unione ma in un luogo comunque soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

3.PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI

Il Considerando 39 è chiaro ed esplicito nell'enunciare che qualsiasi trattamento di dati personali dovrebbe essere lecito e corretto e che le modalità con le quali sono raccolti, utilizzati e consultati tali dati dovrebbe essere trasparenti per le persone fisiche. Il principio di trasparenza così enunciato – il quale riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento stesso – impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro.

3.1 Principio di liceità e correttezza

Come appena visto, i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (art. 5 parag. 1 lett. a) Regolamento).

Affinché possa essere considerato lecito è necessario che il trattamento soddisfi alcuni requisiti che si andranno a trattare nel corso del presente paragrafo e che qui si elencano succintamente:

- √ Consenso;
- √ Esecuzione di un contratto o di misure precontrattuali;
- √ Adempimento di un obbligo legale cui è soggetto il titolare del trattamento;
- √ Salvaguardia di interessi vitali;
- √ Esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri;
- √ Interesse legittimo prevalente di un titolare o di un terzo;

In primo luogo è necessario che il trattamento sia fondato sul consenso dell'interessato o su un'altra base legittima prevista per legge dal Regolamento, dal diritto dell'Unione o da quello degli Stati membri, tenuto conto della necessità di ottemperare all'obbligo legale al quale il titolare del trattamento è soggetto o della necessità di esecuzione di un contratto di cui l'interessato è parte o di esecuzione di misure precontrattuali adottate su richiesta dello stesso. L'interessato deve quindi esprimere il consenso al trattamento dei propri dati personali per una o più specifiche finalità. Il titolare del trattamento dovrebbe essere in grado di dimostrare che l'interessato ha acconsentito al trattamento. In particolare, si legge nel Considerando 42, nel contesto di una dichiarazione scritta dovrebbero esistere garanzie che assicurino, al contempo, che l'interessato sia consapevole di esprimere un consenso e la misura in cui ciò avviene. È necessario pertanto

che il titolare del trattamento predisponga – in ossequio a quanto disposto dalla Direttiva 93/13/CEE – una dichiarazione di consenso che abbia una forma comprensibile e facilmente accessibile, usi un linguaggio semplice e chiaro e che non contenga clausole abusive: che sia, in altre parole, inequivocabile. Il titolare dovrebbe altresì verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato[5]. L'interessato, prosegue il legislatore, dovrebbe essere messo in condizione di conoscere almeno l'identità del titolare del trattamento e delle finalità del trattamento cui i suoi dati personali sono destinati. Questo è importante perché, qualora l'interessato non sia in grado di operare una scelta autenticamente libera – ovvero non gli sia data la possibilità di rifiutare o revocare il consenso senza subire alcun pregiudizio – il consenso non può essere considerato come liberamente espresso. Altresì non potrà essere considerato liberamente espresso[6] se non è data la possibilità all'interessato di esprimere un consenso separato a distinti trattamenti di dati personali[7] o ancora se l'esecuzione di un contratto, compresa la prestazione di un servizio, sia subordinata al consenso sebbene questo non sia necessario per tale esecuzione. Si ricorda nuovamente come il consenso debba essere libero, specifico, informato e inequivocabile e come pertanto non sia ammesso il consenso tacito o presunto; questo comporta, ad esempio, l'impossibilità di utilizzo di moduli con caselle pre-spuntate.

Così come per le altre categorie di dati, anche per i "dati sensibili"[8] il consenso deve essere esplicito; lo stesso vale per il consenso a decisioni basate su trattamenti automatizzati, compresa la profilazione[9]. Tale categoria di dati gode, per espressa previsione, di una speciale protezione dato che per loro natura sono particolarmente – si perdonerà il bisticcio di parole – sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali. Una breve specificazione deve essere fatta con riferimento alle fotografie. Il loro

---

[5] Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante (art. 7 co. 2).

[6] Il legislatore, al riguardo, "presume" la non libertà.

[7] Si pensi alle diverse ipotesi in cui i dati vengono utilizzati a scopi pubblicitari direttamente dal titolare del trattamento o da aziende terze cui il titolare trasmette – grazie al consenso dell'interessato – i dati personali in proprio possesso, intendendo per tali tutte le informazioni che identificano (o rendono identificabile) una persona fisica e che possono fornire dettagli sulle sue caratteristiche, le abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc.

[8] Per "dati sensibili" si devono intendere quelli idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale.

[9] Per "profilazione" si intende «Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica» (art. 4 co. 1 n. 4)). È opportuno, si legge nel Considerando 71, che sia consentito adottare decisioni sulla base di un trattamento automatizzato produttivo di effetti giuridici nei confronti dell'interessato o che comunque incidano significativamente sulla sua persona – il che comprende anche la profilazione solo se espressamente previsto dal diritto dell'Unione europea o degli Stati membri cui è soggetto il titolare del trattamento, anche a fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale secondo i regolamenti, le norme e le raccomandazioni delle istituzioni dell'Unione o degli organismi nazionali di vigilanza e a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento, o se è necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, o se l'interessato ha espresso il proprio consenso esplicito. In ogni caso, prosegue il Considerando, tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione. Tale misura, si raccomanda da ultimo il legislatore, non dovrebbe riguardare un minore.

trattamento non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di "dati biometrici" soltanto quando vengono trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca d una persona fisica o la sua autenticazione. Tornando invece alla speciale protezione accordata ai dati sensibili, vige nei loro confronti un generale divieto di trattamento (art. 9 parag. 1 Regolamento), il quale viene meno nelle seguenti ipotesi:

√ l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;

√ il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

√ il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

√ il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

√ il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

√ il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

√ il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Inoltre, è effettuato sempre per motivi di interesse pubblico, così come evidenziato dal Considerando 55, anche il trattamento di dati personali a cura di autorità pubbliche allo scopo di realizzare fini, previsti dal diritto costituzionale o dal diritto internazionale pubblico, di associazioni religiose ufficialmente riconosciute. Ancora, questa volta secondo il Considerando 56, il trattamento per interesse pubblico di dati raccolti in occasione di attività elettorali a opera dei partiti politici può essere consentito, a patto che vengano predisposte garanzie adeguate.

Il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al

contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3, al quale si rimanda per una trattazione esaustiva dell'argomento. Tale ipotesi viene maggiormente specificata nel Considerando 53, dove si legge che le categorie particolari di dati personali che meritano una maggiore protezione dovrebbero essere trattate soltanto per finalità connesse alla salute, ove necessario per conseguire tali finalità a beneficio delle persone e dell'intera società, in particolare nel contesto della gestione dei servizi e sistemi di assistenza sanitaria o sociale, compreso il trattamento di tali dati da parte della dirigenza e delle autorità sanitarie nazionali centrali a fini di controllo della qualità, informazione sulla gestione e supervisione nazionale e locale generale del sistema di assistenza sanitaria o sociale, nonché per garantire la continuità dell'assistenza sanitaria o sociale e dell'assistenza sanitaria transfrontaliera o per finalità di sicurezza sanitaria, controllo e allerta o a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in base al diritto dell'Unione o nazionale che deve perseguire un obiettivo di interesse pubblico, nonché per studi svolti nel pubblico interesse nell'ambito della sanità pubblica.

Il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica[10], quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale. Il trattamento di categorie particolari di dati personali può infatti essere necessario per motivi di interesse pubblico nei settori della sanità pubblica, anche senza il consenso dell'interessato. Tale trattamento, secondo l'enunciazione fatta dal legislatore nel Considerando 54, dovrebbe essere soggetto a misure appropriate e specifiche a tutela dei diritti e delle libertà delle persone fisiche. Il trattamento dei dati relativi alla salute effettuato per motivi di interesse pubblico, specifica in ultima battuta il Considerando 54, non dovrebbe comportare il trattamento dei dati personali per altre finalità da parte di terzi, quali datori di lavoro, compagnie di assicurazione e istituti di credito.

Il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'art. 89, parag. 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Da ultimo si prevede (art.9 parag. 4 Regolamento) che gli Stati possano mantenere o introdurre ulteriori condizioni e/o limitazioni con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

Con riferimento invece al processo decisionale automatizzato relativo alle persone fisiche, compresa l'attività di profilazione, che produca effetti giuridici nei riguardi dell'interessato o che incida in modo

[10] Nel contesto descritto nel punto i) per "sanità pubblica" si dovrebbero intendere , secondo la definizione del Regolamento (CE) n. 1338/2008 tutti gli elementi relativi alla salute, ossia lo stato di salute, morbilità e disabilità incluse, i determinanti aventi un effetto su tale stato di salute, le necessità in materia di assistenza sanitaria, le risorse destinate all'assistenza sanitaria, la prestazione di assistenza sanitaria e l'accesso universale a essa, la spesa sanitaria e il relativo finanziamento e le cause di mortalità.

analogo significativamente sulla sua persona, l'interessato ha diritto di non esservi sottoposto (art. 22 parag. 1). Ciò però non avviene qualora la decisione:

√ sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;

√ sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;

√ si basi sul consenso esplicito dell'interessato.

Una considerazione a parte si rende necessaria in tema di consenso rilasciato da un minore in relazione ai servizi della società dell'informazione[11]. I minori – come lo stesso legislatore ben evidenzia – possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia nonché dei loro diritti in relazione al trattamento dei dati personali. Questa specifica protezione dovrebbe riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore. Il legislatore sul punto è molto chiaro: il trattamento è lecito se il minore ha almeno sedici anni, in caso contrario dovrà essere prestato o autorizzato da colui che esercita la responsabilità genitoriale[12]. Tuttavia, questo non è necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente a un minore.

Attenzione: il consenso, raccolto precedentemente al 25 Maggio 2018, resta valido se ha tutte le caratteristiche sopra enunciate. In caso contrario sarà opportuno adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati secondo le prescrizioni del regolamento.

Secondo elemento, in forza del quale il trattamento può essere considerato lecito, è che lo stesso sia raccolto in esecuzione di un contratto o di misure precontrattuali, vale a dire che sia necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso.

Terzo elemento è l'adempimento di un obbligo legale al quale è soggetto il titolare del trattamento.

Quarto elemento è che il trattamento sia necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica. Questo è ciò che il Considerando 46 chiama "un interesse essenziale per la vita dell'interessato o di un'altra persona fisica". Il trattamento dei dati fondato su untale interesse dovrebbe aver luogo, in principio, unicamente quando non può essere manifestamente fondato su un'altra base giuridica.

[11] Si pensi ad esempio all'apertura di un account e-mail o di un profilo su un social network.
[12] Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai tredici anni. Il titolare del trattamento deve adoperarsi in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili. Quanto previsto in tema di rilascio del consenso da parte di un minore non pregiudica le disposizioni interne di ciascun Stato membro in materia di contratti; ciò a dire che non incidono sulle norme relative alla validità, formazione o efficacia di un contratto rispetto a un minore. Pertanto, il fatto che un minore infrasedicenne abbia rilasciato un'autorizzazione che non avrebbe potuto rilasciare, non comporta necessariamente l'invalidità del contratto a cui l'autorizzazione si riferisce.

Non si esclude, però, che alcun tipi di trattamento possano rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato; è il caso, ad esempio, del trattamento necessario a fini umanitari per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o ancora in casi di emergenze umanitarie come in occasione di catastrofi di origine naturale o umana.

Si rileva però come una tale base giuridica possa trovare applicazione solamente qualora nessuna delle altre condizioni di liceità sia applicabile.

Ancora, il trattamento deve essere necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Questo è il quinto elemento di liceità del trattamento. A tal proposito il Considerando 45 specifica come, pur dovendo il trattamento essere basato sul diritto dell'Unione o di uno Stato membro, il Regolamento non imponga che vi sia un atto legislativo specifico per ogni singolo trattamento. Un atto legislativo, pertanto, può essere sufficiente come base per più trattamenti. Così come la finalità del trattamento dovrebbe essere stabilita dal diritto dell'Unione o da quello degli Stati membri, anche la scelta del soggetto cui spetta l'esecuzione del compito dovrebbe competere a questi; essi dovrebbero stabilire se il titolare del trattamento che esegue un computo svolto nel pubblico interesse o per l'esercizio di pubblici poteri debba essere una pubblica autorità o altra persona fisica o giuridica di diritto pubblico o, qualora sia nel pubblico interesse, anche per finalità inerenti alla salute (salute pubblica, protezione sociale, gestione dei servizi di assistenza sanitaria), un'associazione di diritto privato come ad esempio un'associazione professionale.

Il sesto e ultimo elemento necessario affinché il consenso possa ritenersi lecito è la necessità del trattamento «per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore». Ad esempio, potrebbero sussistere tali legittimi interessi quando esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, come nel caso in cui l'interessato sia un cliente oppure si trovi alle dipendenze del titolare del trattamento. In ogni caso, l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine. Gli interessi e i diritti fondamentali dell'interessato, continua il legislatore europeo nel Considerando 47, potrebbero in particolare prevalere sugli interessi del titolare del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati personali. Posto che spetta al legislatore prevedere per legge la base giuridica che autorizza le autorità pubbliche a trattare i dati personali, la base giuridica per un legittimo interesse del titolare del trattamento non dovrebbe valere per il trattamento effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti. Costituisce parimenti legittimo interesse del titolare del trattamento interessato trattare dati personali strettamente necessari a fini di prevenzione delle frodi. Può essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto. Ancora, può essere considerato legittimo interesse, secondo quanto esposto nel Considerando 48, quello dei titolari del trattamento facenti parte di un gruppo imprenditoriale o di enti collegati a un organismo centrale che vogliano trasmettere dati personali all'interno del gruppo imprenditoriale a fini amministrativi interni, compreso il trattamento di dati personali dei clienti o dei dipendenti. Si ricorda che sono fatti salvi i principi generali per il trasferimento di dati personali, all'interno di un gruppo imprenditoriale, verso un'impresa

situata in un paese terzo. Ulteriore interesse legittimo può essere considerato quello esemplificato nel successivo Considerando 49, vale a dire il trattare dati personali relativi al traffico, in misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione, vale a dire la capacità di una rete o di un sistema d'informazione di resistere, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi e la sicurezza dei relativi servizi offerti o resi accessibili tramite tali reti e sistemi da autorità pubbliche, organismi di intervento in caso di emergenza informatica (CERT), gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), fornitori di reti e servizi di comunicazione elettronica e fornitori di tecnologie e servizi di sicurezza. Ciò potrebbe, ad esempio, includere misure atte a impedire l'accesso non autorizzato a reti di comunicazioni elettroniche e la diffusione di codici maligni, e a porre termine agli attacchi da «blocco di servizio» e ai danni ai sistemi informatici e di comunicazione elettronica.

Il Considerando 50, invece, anticipa quanto poi disposto al Regolamento circa il trattamento dei dati personali per finalità diverse rispetto a quelle perle quali i dati sono stati inizialmente raccolti. Un simile trattamento dovrebbe essere consentito solo se compatibile con le finalità originarie. In tal caso non è richiesta alcuna base giuridica separata e ulteriore rispetto a quella che ha consentito la raccolta dei dati. Se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento, il diritto dell'Unione o degli Stati membri può stabilire e precisare le finalità e i compiti per i quali l'ulteriore trattamento è considerato lecito e compatibile. L'ulteriore trattamento a fini di archiviazione nel pubblico interesse, o di ricerca scientifica o storica o a fini statistici dovrebbe essere considerato un trattamento lecito e compatibile. La base giuridica fornita dal diritto dell'Unione o degli Stati membri per il trattamento dei dati personali può anche costituire una base giuridica per l'ulteriore trattamento. Per accertare se la finalità di un ulteriore trattamento sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento dovrebbe, dopo aver soddisfatto tutti i requisiti per la liceità del trattamento originario, tener conto tra l'altro di ogni nesso tra tali finalità e le finalità dell'ulteriore trattamento previsto, del contesto in cui i dati personali sono stati raccolti, in particolare le ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo; della natura dei dati personali; delle conseguenze dell'ulteriore trattamento previsto per gli interessati; e dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto.

Un'eccezione alla compatibilità alla finalità appena enunciata è rappresentata dal caso in cui l'interessato abbia prestato il suo consenso o il trattamento si basi sul diritto dell'Unione o degli Stati membri importanti obiettivi di interesse pubblico generale. In questo caso il titolare del trattamento dovrebbe poter sottoporre i dati personali a ulteriore trattamento a prescindere dalla compatibilità delle finalità. Ad ogni modo, dovrebbe essere garantita l'applicazione dei principi stabiliti dal presente regolamento, in particolare l'obbligo di informare l'interessato di tali altre finalità e dei suoi diritti, compreso il diritto di opporsi. L'indicazione da parte del titolare del trattamento di possibili reati o minacce alla sicurezza pubblica e la trasmissione dei dati personali pertinenti a un'autorità competente in singoli casi o in più casi riguardanti lo stesso reato o la stessa minaccia alla sicurezza pubblica dovrebbero essere considerate nell'interesse legittimo perseguito dal titolare stesso. Tuttavia, tale trasmissione o l'ulteriore trattamento dei dati personali dovrebbero essere vietati se il

trattamento non è compatibile con un obbligo vincolante di segretezza, di natura giuridica, professionale o di altro genere.

Come più volte evidenziato, i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, meritano una specifica protezione. È di tutta evidenza, infatti, che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali. Tra tali dati personali dovrebbero essere compresi anche i dati personali che rivelano l'origine razziale o etnica[13].

Mentre include i dati idonei a rivelare l'origine razziale o etnica delle persone, il legislatore si preoccupa di specificare che il trattamento delle fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali. Infatti, le fotografie rientrano nella definizione di "dati biometrici" soltanto qualora siano trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica.

Tale tipologia di dati – vale a dire quelli particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali – non dovrebbe essere oggetto di trattamento a meno che questo non sia specificamente consentito dal Regolamento, tenendo altresì presente il fatto che è consentito agli Stati membri, attraverso l'emanazione di specifiche disposizioni sulla protezione dei dati personali adeguare l'applicazione delle norme regolamentari ai fini della conformità a un obbligo legale o dell'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento[14].

È opportuno, infine, prevedere espressamente deroghe al divieto generale di trattare tali categorie particolari di dati personali: può essere il caso, ad esempio, in cui l'interessato esprima un consenso esplicito o in relazione a esigenze specifiche, in particolare se il trattamento è eseguito nel corso di legittime attività di talune associazioni o fondazioni il cui scopo sia permettere l'esercizio delle libertà fondamentali».

Il bilanciamento fra legittimo interesse del titolare (o del terzo) e diritti e libertà dell'interessato non spetta all'Autorità ma è compito dello stesso titolare; si tratta di una delle principali espressioni del **principio di "responsabilizzazione"** introdotto dal nuovo pacchetto protezione dati. L'interesse legittimo del titolare o

---

[13] Si rileva come il legislatore, nel Considerando 51, specifichi che l'utilizzo del termine "origine razziale" all'interno del Regolamento non implichi in alcun modo l'accettazione da parte dell'Unione di teorie che tentano di dimostrare l'esistenza di razze umane distinte.

[14] Dispone l'art. 6 ai parag. 2 e 3 che:

«2. Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui al capo IX.

3. La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita:

a. Dal diritto dell'Unione; o
b. Dal diritto dello Stato membro cui è soggetto il titolare del trattamento

La finalità del trattamento è determinata in tale base giuridica o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX. Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito.»

del terzo deve prevalere sui diritti e le libertà fondamentali dell'interessato per costituire un valido fondamento di liceità[15].

È bene possibile, ed è lo stesso legislatore all'art. 6 parag. 4. a prevederlo, che il titolare voglia procedere a un trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti e che tale trattamento non sia basato né sul consenso dell'interessato né su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, parag. 1[16]. In tal caso, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro:

a. di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;

b. del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento

c. della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10;

d. delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;

e. dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Si introduce, a tal proposito, il concetto di "**trattamento che non richiede l'identificazione**". Si legge nel Considerando 57[17] che se i dati personali trattati dal titolare non consentono l'identificazione di una persona fisica, questi non dovrebbe essere obbligato ad acquisire ulteriori informazioni per identificare l'interessato al solo fine di rispettare una disposizione regolamentare. In una simile ipotesi e qualora possa dimostrare di

[15] Il regolamento chiarisce espressamente che l'interesse legittimo del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei rispettivi compiti.

[16] Vale a dire:

a) la sicurezza nazionale;
b) la difesa;
c) la sicurezza pubblica;
d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;
e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale;
f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari;
g) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate;
h) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere da a), a e) e g);
i) la tutela dell'interessato o dei diritti e delle libertà altrui;
j) l'esecuzione delle azioni civili.

[17] Si suggerisce di consultare, sul punto, anche il Considerando 64.

non essere in grado di identificare l'interessato, il titolare, se possibile, ne informa l'interessato. Quanto esposto è stato normato dal legislatore nell'art. 11[18].

3.2 Principio di trasparenza

Tale principio, che verrà esposto più analiticamente nel successivo capitolo nella veste di "diritto dell'interessato", impone che le informazioni destinate all'interessato (ma anche più genericamente al pubblico) debbano essere facilmente accessibili e di facile comprensione ed espresse con un linguaggio semplice e chiaro. tali informazioni sono essenzialmente relative all'identità del titolare del trattamento e alle finalità del trattamento stesso. In particolare le finalità specifiche del trattamento dovrebbero essere esplicite, legittime e precisate al momento della raccolta. È molto opportuno, sempre in virtù del principio di trasparenza, che gli interessati siano sensibilizzati riguardo ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, oltre che alle modalità con le quali esercitare i propri diritti in materia di trattamento.

3.3 Principio di *accountability*

Il concetto di *accountability*, nato in ambito aziendale, è stato sviluppato dal punto di vista della privacy da The Centre for Information Policy Leadership in un progetto internazionale (denominato IAP - International Accountability project[19]) che ha visto coinvolti, tra gli oltre sessanta partecipanti, anche le Autorità nazionali per la protezione dei dati e il Garante Europeo per la protezione dei dati personali. L'*accountability* è considerata oggi come l'approccio pratico alla privacy e al trattamento dei dati personali. In quest'ottica lo IAP punta allo sviluppo di strumenti che possano essere utilizzati dalle organizzazioni per valutare – e dimostrare alle Autorità Garanti per la protezione dei dati – il grado della propria *accountability*.

Il principio in commento è stato recepito dal Regolamento, in primo luogo, nell'art. 5 il quale dispone che il titolare del trattamento debba essere in grado di dimostrare – attraverso l'adozione di apposite politiche e la predisposizione di misure *ad hoc* – il rispetto dei principi elencati al paragrafo 1[20] e conseguentemente che il trattamento dei dati personali sia stato effettuato conformemente al Regolamento.

---

18 Art. 11 «1. Se le finalità per cui un titolare del trattamento tratta i dati personali non richiedono o non richiedono più l'identificazione dell'interessato, il titolare del trattamento non è obbligato a conservare, acquisire o trattare ulteriori informazioni per identificare l'interessato al solo fine di rispettare il presente regolamento. 2. Qualora, nei casi di cui al paragrafo 1 del presente articolo, il titolare del trattamento possa dimostrare di non essere in grado di identificare l'interessato, ne informa l'interessato, se possibile. In tali casi, gli articoli da 15 a 20 non si applicano tranne quando l'interessato, al fine di esercitare i diritti di cui ai suddetti articoli, fornisce ulteriori informazioni che ne consentano l'identificazione».

19 È possibile avere maggiori informazioni sul progetto collegandosi all'indirizzo www.accountabilityproject.org.

20 Si riportano, schematicamente, i principi: liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza.

Questo è il contenuto che il legislatore ha inteso dare al principio di *accountability*, la cui traduzione italiana in "responsabilizzazione" non è propriamente fedele al reale contenuto del termine anglosassone. Con *accountability*, infatti, si intendono richiamare almeno due accezioni o componenti fondamentali:

- √ Il **dar conto all'esterno** – in particolare al complesso degli *stakeholder* – in modo esaustivo e comprensibile, del corretto utilizzo delle risorse e della produzione di risultati, in linea con gli scopi istituzionali.
- √ L'esigenza di **introdurre logiche e meccanismi di maggiore responsabilizzazione interna** alle aziende e alle reti di aziende relativamente all'impiego di tali risorse e alla produzione dei correlati risultati.

Se da tali accezioni si desume l'aspetto aziendale dell'*accountability*, è ben possibile trasporre un tale concetto anche in ambito pubblicistico, dove è strettamente collegato a quello di trasparenza. In una tale accezione pubblicistica, l'*accountability* si compone di almeno tre elementi:

√ La trasparenza, intesa come garanzia per i cittadini – in quanto utenti del servizio – di completa accessibilità alle informazioni da parte;

√ La responsività, intesa come la capacità di rendere conto di scelte, comportamenti e azioni e di rispondere alle questioni poste dagli *stakeholder*;

√ La *compliance*, intesa come capacità di far rispettare le norme, sia nel senso di finalizzare l'azione pubblica all'obiettivo stabilito nelle leggi, sia nel senso di fare osservare le regole di comportamento degli operatori della Pubblica Amministrazione.

Oltre che dal citato art. 5, il principio di *accountability* è stato recepito dall'art. 24 del Regolamento il quale dispone 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.». È il Considerando 85 a riportare le possibili conseguenze di una violazione dei dati personali; questa infatti, se non affrontata in modo adeguato e tempestivo, può provocare danni materiale, immateriale o addirittura fisici alle persone[21]. Per questo motivo è fondamentale che il titolare – l'art. 33 ne sancisce l'obbligo – notifichi senza ingiustificato ritardo, e ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza, la violazione di dati personali all'autorità di controllo competente; una tale notifica pò essere evitata qualora il titolare del trattamento sia in grado di dimostrare che, conformemente al principio di responsabilizzazione (art. 5 parag. 1) è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. In caso di notifica oltre il

[21] A titolo puramente esemplificativo il Considerando 85 elenca i seguenti danni: perdita del controllo dei dati personali che riguardano gli interessati danneggiati o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

termine delle 72 ore, questa dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

3.4 Privacy by design e privacy by default

Il principio della privacy *by design* richiede che, al fine di tutelare i diritti e le libertà degli interessati in materia di trattamento dei dati personali e garantire il rispetto delle disposizioni del Regolamento, vengano attuate **adeguate misure tecniche e organizzative al momento sia della progettazione che dell'esecuzione del trattamento stesso**. Le misure che il legislatore europeo ritiene essere adottabili al fine di poter dimostrare la conformità del trattamento con il dettato regolamentare sono elencate – ma si tratta di un elencazione puramente indicativa e certamente non esaustiva – nell'art. 25 parag. 1[22] e nel Considerando 78. Queste consistono nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare[23] i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza.

L'applicazione del principio della privacy *by design* richiede anche un coinvolgimento di coloro che sviluppano e progettano prodotti, servizi e applicazioni che comportano, in qualche misura, un trattamento di dati personali. Infatti, in fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i relativi produttori dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppino e progettino tali prodotti, servizi e applicazioni; altresì, tenuto debito conto dello stato dell'arte, i titolari del trattamento e i responsabili del trattamento dovrebbero essere messi nelle condizioni di poter adempiere ai loro obblighi di protezione dei dati. Da ultimo il legislatore europeo, sempre nel Considerando 78, ritiene che i principi della protezione dei dati "fin dalla progettazione" (*by design*) e di *default* dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici.

L'approccio al tema da parte del legislatore è più orientato verso la protezione dei dati piuttosto che dell'interessato e si concretizza in un metodo basato sulla valutazione del rischio (c.d. *risk based approach*), con la quale si determina la misura di responsabilità del titolare o del responsabile del trattamento, tenendo conto della natura, della portata, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà degli utenti. La definizione di "rischio" è contenuta nei Considerando

[22] « 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.».

[23] Secondo la definizione di cui all'art. 4 n. 5) del Regolamento, per "pseudonimizzazione" si deve intendere «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.».

75 e 76, dove vengono indicate le fonti di rischio per i diritti e le libertà delle persone fisiche – aventi probabilità di accadimento e, nel caso, gravità diverse. Nello specifico i potenziali rischi possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare:

- √ Se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo;
- √ Se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano;
- √ Se sono trattati dati sensibili;
- √ In caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione 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, al fine di creare o utilizzare profili personali;
- √ Se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori;
- √ Se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato, prosegue il Considerando 76, dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante la quale si stabilisce se i trattamenti di dati comportino semplicemente un rischio o addirittura un rischio elevato.

Il principio della privacy *by default*[24], invece, prevede che le impostazioni di tutela della vita privata relativi ai servizi e prodotti rispettino i principi generali della protezione dei dati, quali la minimizzazione dei dati e la limitazione delle finalità. Tale principio stabilisce che per impostazione predefinita le imprese dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. Sarà pertanto necessario progettare un sistema di trattamento di dati che garantisca la non eccessività dei dati raccolti.

Tutto questo si enuclea dalla lettura dell'art. 25 parag. 2, nel qual il legislatore dispone che «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.».

[24] Una parte della dottrina sostiene che il concetto di privacy *by default* sia già contenuto in quello di privacy *by design* e che pertanto sarebbe più corretto parlare di principio di minimizzazione (*minimisation*).

La privacy *by default* comporta, da una parte, che in un complessivo approccio di progettazione di sistemi informatici funzionale alla tutela della privacy, determinate informazioni debbano essere protette in modo rafforzato. Dall'altra parte, invece, implica l'utilizzo automatico di determinate impostazioni a maggior tutela dell'interessato, scelte da chi progetta il sistema informatico con la possibilità di cambiamento dell'opzione scelta da parte dell'interessato. L'utilità di queste impostazioni automatiche (c.d. *default settings*) è giustificabile considerando che gli interessati mostrano sempre una certa tendenza a non modificare le impostazioni di default, affidandosi alle impostazioni preimpostate e non condividendo più informazioni di quelle richieste di base.

Pertanto, un titolare del trattamento, al fine di applicare correttamente quanto disposto dall'art. 25, dovrà:

√ Progettare il *default settings* tenendo conto del principio del "*would have wanted standard*", secondo il quale le scelte di progettazione vanno compiute tenendo in considerazione ciò che un utente ben informato sceglierebbe e ne avesse la possibilità;

√ Attuare il principio della minimizzazione, vale a dire non trattate dati ulteriori a quelli strettamente necessari per perseguire le singole finalità;

√ Garantire che i dati raccolti non siano conservati per tempi ulteriori rispetto a quelli minimi necessari;

√ Assicurarsi che l'accesso a un numero indefinito di dati personali da parte di macchine ("senza l'intervento della persona fisica") non sia possibile.

Da non sottovalutare, da ultimo, il regime sanzionatorio correlato all'inosservanza dell'art. 25. La sanzione amministrativa pecuniaria applicabile può arrivare fino a €. 10.000.000,00, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. La sanzione si applica al titolare o al responsabile del trattamento sui quali, quindi, grava l'obbligo di verificare il rispetto dell'art. 25 anche con riferimento ai software o ai sistemi dei propri fornitori.

4.DIRITTI DELL'INTERESSATO

4.1 Informazioni, comunicazioni e modalità per l'esercizio dei diritti dell'interessato

Il legislatore europeo detta, all'art. 12, alcuni criteri affinché gli interessati possano esercitare più agevolmente i diritti riconosciuti loro dal Regolamento (UE) 2016/679.

Il titolare del trattamento dovrà adottare misure adeguate per fornire all'interessato tutte le informazioni elencate agli artt. 13 e 14 – il cui contenuto verrà analizzato tra poco – e le comunicazioni di cui agli artt. 15-22 e 34 relative al trattamento, in forma concisa, trasparente, intelligibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. In questo modo può essere rispettato il principio della trasparenza. Le misure adeguate possono concretizzarsi anche nel fornire le informazioni di cui sopra in formato elettronico, ad esempio nel caso in cui siano destinate al pubblico attraverso un sito web; in ogni caso sono fornite per iscritto o con altri mezzi. Tali informazioni possono addirittura essere fornite, se richiesto dall'interessato, anche oralmente purché sia comprovata con altri mezzi la sua identità.

Il contenuto dell'informativa sarà differenziato a seconda che i dati siano (art. 13) o meno (art. 14) raccolti presso l'interessato. Nel primo caso, il titolare del trattamento fornisce all'interessato nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

a) L'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;

b) I dati di contatto del responsabile della protezione dei dati, ove applicabile;

c) Le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

d) Qualora il trattamento sia necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, dovrà essere fornito tale legittimo interesse;

e) Gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

f) Ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'art. 46 o 47, o all'art. 49 co. 2, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

In aggiunta a tali informazioni, per garantire un trattamento corretto e trasparente, il titolare del trattamento dovrà fornire anche le seguenti informazioni:

g) Il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

h) L'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

i) L'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca, qualora l'interessato abbia espresso il consenso al trattamento per una o più specifiche finalità.

j) Il diritto di proporre reclamo a un'autorità di controllo;

k) Se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

l) L'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Tutte le informazioni appena elencate vanno fornite se e nella misura in cui l'interessato già non ne disponga e, qualora il titolare intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento deve fornire all'interessato le informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente e necessaria per garantire un trattamento corretto e trasparente (punti da g) a l)).

Nel secondo caso, vale a dire qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento gli fornisce le seguenti informazioni, elencate all'art. 14:

a) L'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;

b) I dati di contatto del responsabile della protezione dei dati, ove applicabile;

c) Le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

d) Le categorie di dati personali in questione;

e) Gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

f) Ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'art. 46 o 47, o all'art. 49, co. 2, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

Come nel precedente, anche in questo caso il titolare, in aggiunta alle informazioni appena elencate, al fine di garantire un trattamento corretto e trasparente, dovrà fornire anche le seguenti informazioni:

g) Il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

h) Qualora il trattamento sia necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, dovrà essere fornito tale legittimo interesse;

i) L'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

j) Qualora l'interessato abbia espresso il suo consenso al trattamento per una o più specifiche finalità, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;

k) Il diritto di proporre reclamo a un'autorità di controllo;

l) La fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;

m) L'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Tutte le informazioni appena elencate (lettere a)-m)) dovranno essere fornite dal titolare:

a) Entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;

b) Al più tardi al momento della prima comunicazione all'interessato, nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato; oppure

c) Non oltre la prima comunicazione dei dati personali, nel caso sia prevista la comunicazione ad altro destinatario.

Come nel caso precedente, qualora il titolare intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento deve fornire all'interessato le informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente e necessaria per garantire un trattamento corretto e trasparente (punti da g) a m)).

Tutto quanto finora esposta non si applica se e nella misura in cui:

a) L'interessato dispone già delle informazioni;

b) Comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato[25];

c) L'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure

d) Qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge.

4.2 Diritto di accesso dell'interessato

Il legislatore europeo, all'art. 15, dispone che l'interessato possa accedere ai dati personali che lo riguardano che sono stati raccolti dal titolare e che possa farlo a intervalli ragionevoli, in modo tale da essere consapevole del trattamento cui essi sono sottoposti e verificarne la liceità. Pertanto il titolare, dietro semplice richiesta, dovrà fornire all'interessato le seguenti informazioni:

a) Le finalità del trattamento;

b) Le categorie di dati personali oggetto di trattamento;

c) I destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali. In quest'ultimo caso, vale a dire qualora i dati personali siano trasferiti a un paese terzo o a un organizzazione internazionale, l'interessato ha il diritto di essere informato circa l'esistenza di garanzie adeguate relative al trasferimento, per le quali si rimanda all'art. 46 del Regolamento (UE) 2016/679.

d) Quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e) L'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento di quelli che lo riguardano o di opporsi al loro trattamento;

f) Il diritto di proporre reclamo a un'autorità di controllo;

g) Qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h) L'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4[26] e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

---

[25] In particolare, per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;

Per quanto riguarda la fornitura in concreto delle informazioni, qualora l'interessato ne faccia richiesta attraverso mezzi elettronici, il titolare dovrà fornirle in un formato elettronico di uso comune. Alternativamente potranno essere richieste per iscritto e il titolare ne fornirà copia su supporto cartaceo; la prima copia sarà gratuita mentre per le ulteriori eventuali copie potrà essere addebitato un contributo spese ragionevole basato sui costi amministrativi (art. 15 parag. 3).

Per meglio garantire un tale diritto di accesso il legislatore, nel Considerando 63, evidenzia che, ove possibile, il titolare dovrebbe consentire all'interessato l'accesso da remoto (vale a dire direttamente dal proprio pc, tablet o smartphone) per consultare autonomamente i propri dati personali. Ovviamente, come previsto dall'art. 15 parag. 4, il diritto dell'interessato di ottenere una copia non deve ledere i diritti e le libertà altrui – compreso il segreto industriale, quello aziendale e la proprietà intellettuale – segnatamente i diritti d'autore che tutelano il software.

Il diritto di accesso è riconosciuto altresì dal D.lgs n. 196/2003 (c.d. Codice della Privacy), agli artt. 7 e ss., secondo il quale le relative istanze devono essere riscontrate "senza ritardo" al massimo entro quindici giorni, elevabili a trenta in casi di particolare complessità. Se il riscontro non avviene nei tempi previsti, o non è soddisfacente, l'interessato è abilitato a presentare ricorso al Garante Privacy, il quale potrà prendere i provvedimenti più opportuni. Per questo motivo è consigliabile che il titolare del trattamento approntì una struttura quanto più funzionale ed efficiente per monitorare costantemente il ricevimento delle istanze di accesso e fornisca adeguate istruzioni a incaricati e responsabili circa la gestione ed evasione delle stesse entro i brevi termini previsti dal legislatore.

Le istanze di accesso non richiedono particolari requisiti di forma e il Garante per la Protezione dei dati personali ha pubblicato sul proprio sito internet un modello (indicativo) per agevolare gli interessati nell'esercizio dei loro diritti[27]. Si specifica che nei casi previsti dall'art. 7 co. 1 e 2 Codice Privacy, le istanze possono essere anche presentate oralmente, vale a dire quando l'interessato chieda:

- √ La conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile;
- √ L'origine dei dati personali;
- √ Le finalità e le modalità del trattamento;
- √ La logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
- √ Gli estremi identificativi del titolare, dei responsabili e del rappresentante designato;

---

[26] Il paragrafo 1 dispone che «L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.».
Il paragrafo 4, al quale si rimanda per la lettura completa dei riferimenti normativi, dispone che «Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.».

[27] Il modello è scaricabile all' indirizzo
http://194.242.234.211/documents/10160/10704/MODELLO+esercizio+diritti+in+materia+di+protezione+dei+dati+personali.pdf

- √ L'indicazione dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

Nei casi appena elencati la richiesta viene annotata sinteticamente a cura dell'incaricato o del responsabile.

Il titolare dovrà verificare l'identità del titolare. A tale scopo il Codice prevede che essa possa essere verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento. Se l'interessato si avvale di un rappresentante/delegato questi dovrà esibire o allegare copia della procura ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato. Questi adempimenti, si specifica, non possono essere estesi all'esercizio di opposizione al trattamento per finalità di marketing, ove costituirebbero un inutile aggravio e una decisa sproporzione non consentita della normativa.

4.3 Diritto di rettifica, all'oblio e di limitazione di trattamento

I successivi artt. 16, 17, 18 prevedono ulteriori importanti diritti (rettifica, oblio, limitazione di trattamento) già conosciuti dal nostro ordinamento essendo contenuti nel D.lgs n. 196/2003.

Ci si sofferma in particolare sul **diritto all'oblio** in quanto, vero che già noto ma finalmente riconosciuto anche dal legislatore e non solo dalla giurisprudenza. Anche in relazione al diritto all'oblio siamo sprovvisti di una definizione normativa e dobbiamo pertanto chiedere aiuto alla dottrina e alla giurisprudenza, secondo le quali, tradizionalmente, rileviamo l'esistenza di tre accezioni di "diritto all'oblio". La prima lo identifica con il diritto di un soggetto a non rendere noti dati attinenti la propria persona per accadimenti legittimamente pubblicati e rispetto ai quali è passato un notevole lasso di tempo. La seconda accezione, invece, non fa riferimento al tempo trascorso tra la prima pubblicazione dell'informazione e la sua ripubblicazione ma al tempo che la notizia è stata online (e quindi visibile al pubblico). Da ultimo, la terza accezione si riferisce al diritto alla rettifica e alla cancellazione dei dati personali o all'opposizione al trattamento degli stessi. In una delle ultime sentenza della Corte di Giustizia sul tema[28] i giudici hanno scritto le motivazioni prendendo a riferimento proprio quest'ultima accezione. La sentenza non crea una nuova definizione di diritto all'oblio, ma sancisce il diritto di un soggetto a non essere "trovato" online; non potranno essere cancellati i dati presso il titolare, afferma la Corte, ma soltanto il collegamento a tali dati, facendo gravare l'obbligo di rimozione del link solo sul motore di ricerca.

[28] Sentenza del 13.05.2014 Causa C-131/12, nella quale la Corte ha constatato che «esplorando Internet in modo automatizzato, il gestore di un motore di ricerca «raccoglie» dati ai sensi della Direttiva 95/46/CE. Il gestore «estrae», «registra» e «organizza» tali dati nell'ambito dei suoi programmi di indicizzazione, prima di «metterli a disposizione» dei propri utenti sotto forma di elenchi di risultati. Un trattamento di dati personali effettuato da un siffatto gestore consente a qualsiasi utente di Internet, allorché effettua una ricerca a partire dal nome di una persona fisica, di ottenere, mediante l'elenco di risultati, una visione complessiva strutturata delle informazioni relative a questa persona su Internet. Qualora si constati, in seguito a una richiesta della persona interessata, che l'inclusione di tali link nell'elenco è, allo stato attuale, incompatibile con la Direttiva, le informazioni e i link figuranti in tale elenco devono essere cancellati.».

L'interessato ha ora pertanto il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali erano stati raccolti; a tale diritto corrisponde l'obbligo del titolare di cancellarli senza ingiustificato ritardo. Se è vero che l'interessato ha diritto a vedere cancellati i propri dati, questo può avvenire solo in ipotesi determinate ed elencate all'art. 17 parag. 1, vale a dire qualora:

a) I dati personali non siano più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b) L'interessato revochi il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;

c) L'interessato si opponga al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussista alcun motivo legittimo prevalente per procedere al trattamento, oppure si opponga al trattamento ai sensi dell'articolo 21, paragrafo 2;

d) I dati personali siano stati trattati illecitamente;

e) I dati personali debbano essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

f) I dati personali siano stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

Un tale diritto assume una particolare rilevanza, come si legge nel Considerando 65, se il consenso è stato prestato dall'interessato quando era minore e quindi non pienamente consapevole dei rischi derivanti dal trattamento e, una volta, raggiunta la maggiore età, voglia eliminare tale tipo di dati personali, in particolare da internet. Ad ogni buon grado l'interessato può esercitare tale diritto indipendentemente dal fatto che non sia più un minore. Tuttavia, secondo quanto affermato nel Considerando 65 e trasferito nell'art. 17 parag. 3, l'ulteriore conservazione dei dati personali dovrebbe essere lecita qualora risulti necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria.

Il Considerando 66 attribuisce un'ulteriore e importante incombenza al titolare del trattamento – recepita dall'art. 17 parag. 3 – vale a dire informare gli altri titolari che trattano i dati oggetto di cancellazione di cancellare qualsiasi collegamento con tali dati o copia di essi. Per fare ciò è opportuno che il titolare del trattamento adotti le misure ragionevoli tenendo conto della tecnologia disponibile, dei costi di attuazione, dei mezzi a sua disposizione, comprese misure tecniche, per informare della richiesta dell'interessato i titolari del trattamento che trattano i dati personali. In questo modo, è opinione del legislatore europeo, è possibile rafforzare il diritto all'oblio nell'ambiente online.

Solo brevemente si trattano gli altri diritti dell'interessato elencati all'inizio del paragrafo, in quanto già conosciuti nel nostro ordinamento. Per quanto riguarda il **diritto di rettifica** (art. 16), l'interessato «ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.». Con riferimento, invece, al **diritto di limitazione del trattamento** (art. 18) le modalità per limitare concretamente il trattamento potrebbero consistere, tra l'altro, nel trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento, nel rendere i dati personali selezionati inaccessibili agli utenti o nel rimuovere temporaneamente i dati pubblicati su un sito web. Negli archivi automatizzati, la limitazione del trattamento dei dati personali dovrebbe, in linea di massima, essere assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano essere più modificati. Il sistema, altresì, dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato.

4.4 Diritto alla portabilità dei dati

Una delle novità introdotte dal Regolamento in tema di diritti dell'interessato, è la possibilità di ricevere i dati personali che si sono forniti a un titolare del trattamento e di trasmetterli ad altro titolare senza impedimenti da parte del primo. Il nuovo diritto alla portabilità – diversamente dal diritto di accesso previsto dalla abrogata Direttiva 95/46/CE il quale vincolava la trasmissione delle informazioni richieste al formato utilizzato dal titolare – intende promuovere il controllo degli interessati sui propri dati personali, facilitando la circolazione, la copia o la trasmissione dei dati da un ambiente informativo all'altro; questo sia che si tratti dei propri sistemi, dei sistemi di soggetti terzi fidati ovvero di quelli di un diverso titolare del trattamento.

Il diritto di ricevere un "sottoinsieme" (più avanti si comprenderà l'utilizzo del termine) dei dati personali e di conservarli – sia su supporto personale che su un *cloud* privato – costituisce un'integrazione del diritto di accesso ed è uno strumento con cui gli interessati possono facilmente gestire e riutilizzare i propri dati personali in piena autonomia.

Come anticipato, tale diritto non consente solo di ricevere i dati, ma anche di trasmetterli – o farli trasmettere – ad altro titolare senza impedimenti. L'aspettativa del legislatore è quella che, oltre ad ampliare il margine di controllo dei consumatori, impedendo così forme di "*lock-in*" tecnologico[29], il diritto alla portabilità dei dati possa promuovere l'innovazione e la condivisione di dati personali fra titolari del trattamento in piena sicurezza e sotto il controllo dell'interessato.

Il WP 29 sostiene a riguardo che un tale diritto possa favorire la condivisione controllata e limitata delle informazioni personali fra più soggetti e, conseguentemente, arricchire l'esperienza dell'utente nella fruizione di determinati servizi. I benefici e i rischi legati alla combinazione di dati personali provenienti dai diversi ambiti di attività di una persona emergono con evidenza in rapporto alla c.d. "quantificazione del

[29] Viene definita *lock-in* la situazione per la quale un prodotto o un sistema è vincolato perennemente, per essere utilizzato, a un altro prodotto o sistema.

sé"[30] e all'internet delle cose (I.O.T., I*nternet Of Things*)[31]. La portabilità, inoltre, può favorire la trasmissione e il riutilizzo di dati personali fra più servizi che siano di interesse per il singolo utente.

Il diritto alla portabilità spetta in tutti i casi in cui il trattamento si basi sul consenso espresso dall'interessato per una o più specifiche finalità, qualora sia necessario per l'esecuzione di un contratto[32] ovvero sia effettuato con mezzi automatizzati[33]. Il diritto alla portabilità, pertanto, non è rivendicabile qualora il trattamento si basi su un altro motivo legittimo diverso dal consenso o dal contratto e, per sua stessa natura, non potrà essere esercitato nei confronti di un responsabile del trattamento che tratti dati nell'esercizio delle sue funzioni pubbliche.

Il legislatore ha ritenuto di dover disciplinare, anche in virtù di quanto riportato nel Considerando 68, le modalità di trasmissione dei dati, sancendo all'art. 20 il diritto dell'interessato di ricevere i dati in un formato strutturato, di uso comune (e secondo il considerando anche "interoperabile") e leggibile da dispositivo automatico[34]. Il Considerando 68 aggiunge, come appena accennato, che il formato dovrebbe essere "interoperabile"[35] e che a tal fine gli Stati membri dovrebbero incoraggiare i titolari del trattamento a sviluppare tali formati che facilitino la portabilità dei dati[36].

Considerata l'ampia gamma di dati potenzialmente oggetto di trattamento da parte del titolare, i formati più idonei saranno diversi in rapporto ai singoli settori di attività e già oggi esiste un'importante varietà di formati adeguati. Sempre in tema di formati, il Considerando 68 specifica che «il diritto dell'interessato di

---

[30] La "quantificazione del sé" può essere definita come «la registrazione di ogni aspetto della nostra vita quotidiana, anche e soprattutto di quelli più banali e triviali (il cibo, i libri, l'attività fisica, il sonno), grazie a strumenti più o meno evoluti che permettono di acquisire automaticamente questi dati.»

[31] *Internet Of Things* è l'espressione utilizzata per definire la rete delle apparecchiature e dei dispositivi, diversi dai computer, connessi a Internet: possono essere sensori per il fitness, automobili, radio, impianti di climatizzazione, ma anche elettrodomestici, lampadine, telecamere, container per il trasporto delle merci. Con tale termine, pertanto, si vuole identificare qualunque dispositivo elettronico equipaggiato con un software che gli permetta di scambiare dati con altri oggetti connessi.

[32] Relativamente ai dati dei dipendenti, il diritto alla portabilità trova applicazione, solo in questo caso, vale a dire qualora il trattamento si basi su un contratto di cui l'interessato (vale a dire il dipendente) è parte. Alcuni trattamenti riferiti alla gestione delle risorse umane si fondano sull'interesse legittimo, ovvero sono necessari per adempiere a specifici obblighi di legge in materia di lavoro. In pratica, il diritto alla portabilità nel contesto della gestione del personale potrà indubbiamente trovare applicazione con riguardo a determinati trattamenti (per esempio, in rapporto alla gestione degli stipendi o ai servizi di mobilità interna), ma in molte altre situazioni occorrerà procedere caso per caso così da verificare se siano soddisfatte tutte le condizioni cui soggiace il diritto alla portabilità dei dati.

[33] Ciò significa che il diritto non è esercitabile qualora i dati siano conservati in archivi o registri cartacei.

[34] Nel Considerando 21 della Direttiva 2013/37/UE si rinviene la seguente definizione dell'espressione "leggibile meccanicamente" (*machine readable*): «formato di file strutturato in modo tale che le applicazioni software possano agevolmente identificarlo, riconoscerlo ed estrarne dati specifici. I dati codificati in file strutturati in un formato leggibile meccanicamente sono dati leggibili meccanicamente. I formati leggibili meccanicamente possono essere aperti o proprietari; possono essere standard formali o meno. I documenti codificati in un formato di file che limita il trattamento automatico, poiché l'estrazione dei dati in essi contenuti non è possibile o non avviene con facilità, non dovrebbero essere considerati documenti in formato leggibile meccanicamente. Gli Stati membri dovrebbero, se del caso, promuovere l'impiego di formati aperti leggibili meccanicamente.».

[35] L'UE definisce "interoperabilità" «la capacità di organizzazioni diverse e disparate di interagire in vista di obiettivi comuni concordati e reciprocamente vantaggiosi ricorrendo alla condivisione di conoscenze e informazioni tra le organizzazioni, per mezzo dei processi aziendali che su di esse si basano, tramite lo scambio di dati fra i rispettivi sistemi TIC.» (art. 2 Decisione n. 922/2009/CE del Parlamento europeo e del Consiglio).

[36] Il WP29 sostiene con forza la ricerca di forme di collaborazione fra i produttori e le associazioni di categoria al fine di sviluppare un insieme condiviso di standard e formati interoperabili che soddisfino i requisiti del diritto alla portabilità dei dati. Questa sfida è stata raccolta anche dallo *European Interoperability Framework* (EIF), che ha elaborato un approccio condiviso all'interoperabilità pensato per i soggetti che intendano prestare servizi pubblici in modo congiunto. Limitatamente al suo ambito di applicazione, questo schema specifica una serie di elementi comuni comprendenti un lessico condiviso, concetti, principi, politiche, linee-guida, raccomandazioni, standard, specifiche e prassi (fonte: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf) .

trasmettere o ricevere dati personali che lo riguardano non dovrebbe comportare l'obbligo per i titolari del trattamento di adottare o mantenere sistemi di trattamento tecnicamente compatibili.». Questo significa che con il perseguimento della portabilità si intendono produrre sistemi interoperabili piuttosto che compatibili.

Guardando sempre il fine dell'interoperabilità e conseguentemente della portabilità dei dati, questi dovrebbero essere messi a disposizione con un elevato livello di astrazione rispetto a qualsiasi altro formato a uso interno o proprietario. Di conseguenza, la portabilità comporta un ulteriore livello di trattamento da parte del titolare: questo infatti dovrà adoperarsi per estrarre i dati dalla piattaforma –ecco perché *supra* ho utilizzato il termine "sottoinsieme" – filtrando le informazioni personali che non rientrano nell'ambito della portabilità, come ad esempio i dati dedotti o quelli connessi alla sicurezza di un sistema. Pertanto, il titolare è sollecitato a individuare in precedenza i dati che, nei rispettivi sistemi, ricadono nell'ambito del diritto alla portabilità.

In tema di formato concretamente utilizzabile è intervenuto anche il WP29 il quale, nelle linee guida elaborate sul tema, ha specificato che qualora non vi siano formati di impiego comune in un determinato settore di attività o in un determinato contesto, i titolari dovrebbero fornire i dati personali utilizzando formati aperti di impiego comune (per esempio: .xml, .json, .csv) unitamente a metadati utili, al miglior livello possibile di granularità, mantenendo un livello elevato di astrazione. In tal senso, si dovrebbero utilizzare – prosegue il WP29 – metadati idonei a descrivere con precisione il significato delle informazioni oggetto di transazione. I metadati dovrebbero essere sufficienti a consentire la funzionalità e il riutilizzo dei dati e, ovviamente, non dovrebbero rivelare segreti industriali. Pertanto, fornire all'interessato, per esempio, la versione in formato .pdf delle informazioni contenute nella sua casella di "posta elettronica in arrivo", sarebbe poco conciliabile con il requisito di un formato sufficientemente strutturato o descrittivo, tale da permettere con facilità il riutilizzo dei dati contenuti nella casella di posta. I dati relativi alla posta elettronica dovrebbero essere messi a disposizione dell'utente in un formato che garantisca l'integrità di tutti i metadati in modo da consentirne l'effettivo ed efficace riutilizzo. In tal senso, nella scelta del formato, il titolare dovrebbe valutare in che modo questo possa ostacolare o incidere sul diritto dell'interessato al riutilizzo dei dati forniti. Se il titolare è in grado di offrire più opzioni all'interessato quanto al formato preferito per i dati personali portabili, dovrebbe essere prevista anche un'informativa chiara sugli effetti prodotti dalle singole opzioni. D'altro canto, non è possibile fondare legittimamente il trattamento di ulteriori metadati esclusivamente sul presupposto di una loro necessità o utilità ai fini dell'adempimento di un'eventuale richiesta di portabilità.

Il WP29 si preoccupa inoltre di suggerire – in modo da agevolare i titolari nell'adempimento dell'obbligo ex art. 5 parag. 1 lett. f)[37] – delle strategie in tema di sicurezza dei dati portabili. Infatti, dal momento che la portabilità mira a trasportare dati personali all'esterno del sistema informativo del titolare, la fase di trasmissione è fonte di un potenziale rischio per la sicurezza dei dati, soprattutto in termini di loro violazione. Il titolare ha la responsabilità dell'adozione di tutte le misure di sicurezza necessarie a garantire non soltanto la trasmissione sicura dei dati personali – attraverso la crittografia *end-to-end* – al destinatario corretto, ma

[37] Il titolare deve garantire la «adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.».

anche la permanente tutela dei dati personali che rimangono nel suo sistema, oltre a procedure trasparenti per la gestione di eventuali violazioni dei dati, in conformità alla Direttiva (UE) 2016/1148. Per fare questo i titolari dovrebbero compiere una valutazione dei rischi specificamente legati alla portabilità dei dati e adottare di conseguenza le misure idonee per limitarli. Tali misure potrebbero consistere, qualora fosse già necessario procedere all'autenticazione dell'interessato, nel ricorso a ulteriori misure di autenticazione, come ad esempio una "domanda segreta" ovvero a un ulteriore fattore di autenticazione quale potrebbe essere una password monouso; ancora, se vi fosse motivo di sospettare una compromissione dell'account, si potrebbe ricorrere alla sospensione o al congelamento della trasmissione; da ultimo, un'ulteriore misura adottabile potrebbe essere – nel caso di trasmissione diretta da un titolare a un altro – quella di ricorrere a meccanismi di "autenticazione delegata" come quella attuabile attraverso un token. Ovviamente tali misure, come ricorda giustamente il WP29, non devono avere natura ostativa e non devono ostacolare l'esercizio dei diritti da parte degli utenti, ad esempio gravandoli di costi ulteriori. Il titolare che risponde a una richiesta di portabilità è, come appena visto, responsabile della sicurezza dei dati durante la trasmissione, mentre non lo è del trattamento effettuato dal singolo interessato o da un'altra società ce riceva i dati in questione. Essi, infatti, agiscono per conto dell'interessato, anche se i dati personali sono trasmessi direttamente a un diverso titolare; pertanto il titolare non è responsabile dell'osservanza delle norme in materia di protezione dei dati da parte del titolare ricevente, dal momento che questi non viene selezionato da lui.

Un altro ambito del quale il titolare che risponde a una richiesta di portabilità non ha alcun obbligo specifico è quello della verifica della qualità dei dati prima della loro trasmissione (è invero ovvio che i dati dovrebbero già rispettare i requisiti di esattezza e aggiornamento in ossequio ai principi fissati nell'art. 5 parag. 1 del Regolamento). Inoltre, il diritto alla portabilità non impone al titolare alcun obbligo di conservazione dei dati per un periodo superiore al necessario ovvero superiore a quello eventualmente specificato, ma soprattutto non lo impone al solo scopo di adempiere a una potenziale richiesta di portabilità.

Determinati obblighi ricadono, al contrario, in capo al titolare ricevente, vale a dire a colui il quale riceve dati personali e seguito di una richiesta di portabilità presentata dall'interessato a un altro titolare; questi (il ricevente) infatti è tenuto a garantire che i dati forniti siano pertinenti e non eccedenti rispetto al nuovo trattamento svolto, ma contemporaneamente non è tenuto ad accettare e trattare i dati personali trasmessi a seguito di una richiesta di portabilità. Ancora, il ricevente assume il ruolo di titolare nei riguardi dei dati personali trasmessi ed è tenuto all'osservanza dei principi fissati nell'art. 5 del Regolamento[38], con la conseguenza che dovrà specificare con chiarezza le finalità di ogni nuovo trattamento prima che sia formulata la richiesta di trasmissione diretta dei dati portabili, conformemente con i requisiti di trasparenza di cui all'art. 12[39]. In aggiunta dovrebbe astenersi dal trattare dati personali che non siano pertinenti e il trattamento dovrebbe essere limitato ai dati necessari perle nuove finalità anche se i dati personali in questione fanno parte di un più ampio insieme di dati trasmessi attraverso una procedura di portabilità.

Il problema della sicurezza dei dati non coinvolge solo il titolare del trattamento, ma anche gli stessi interessati che esercitano il diritto alla portabilità. Infatti, una volta recuperati i propri dati personali è molto

[38] I principi, che qui si riportano sinteticamente come promemoria, sono: liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, integrità e riservatezza, conservazione limitata e responsabilizzazione.
[39] Si veda *supra* paragrafo 4.2.

probabile che gli interessati li conservino in sistemi meno sicuri rispetto a quello del titolare. Nonostante l'interessato che chiede di ricevere informazioni abbia la responsabilità di individuare le misure corrette al fine di garantire la sicurezza dei propri dati all'interno del proprio sistema, dovrebbe anche essere sensibilizzato al riguardo, in modo da adoperarsi per tutelare le informazioni ricevute. La prassi che il WP29 consiglia di adottare al titolare a tal fine è quella di raccomandare l'impiego di formati idonei, di strumenti di crittografia e di altre misure di sicurezza al fine di facilitare l'interessato nel compito.

Per concludere sul tema della portabilità si specifica, seguendo quanto già disposto dal legislatore europeo nell'art. 20 parag. 4, che l'esercizio di un tale diritto – così come di qualsiasi altro diritto riconosciuto ai sensi del Regolamento (UE) 2016/679 – non pregiudica nessuno degli altri diritti. L'interessato, infatti, può continuare a usufruire del servizio offerto dal titolare anche dopo aver richiesto la portabilità dei propri dati. Questa infatti non comporta l'automatica cancellazione dei propri dati conservati nei sistemi del titolare – una siffatta operazione soggiace alle regole stabilite nell'art. 17 – né incide sul periodo di conservazione preciso originariamente per i dati oggetto di trasmissione. L'interessato può pertanto continuare a esercitare i diritti riconosciuti dal Regolamento fintanto che prosegue il trattamento effettuato da titolare.

Per quanto riguarda la tipologia dei dati portabili questi devono rispettare due condizioni: che siano dati personali riguardanti l'interessato e che sia stato egli stesso a fornirli. La prima condizione comporta che la richiesta non possa applicarsi né ai dati anonimi[40] né a quelli non concernenti l'interessato.

Con riferimento alla seconda condizione, ossia al fatto che i dati siano stati forniti dall'interessato, può essere fatta una distinzione fra le varie categorie di dati in rapporto alla rispettiva origine per stabilire se si applichi il diritto alla loro portabilità. Possono quindi essere ulteriormente individuati i dati forniti consapevolmente e attivamente dall'interessato (indirizzo postale, nome utente, età, ecc) e quelli forniti attraverso la fruizione di un servizio o l'utilizzo di un dispositivo (ad esempio la cronologia delle ricerche effettuate, i dati relativi al traffico, i dati relativi all'ubicazione nonché atri dati grezzi come la frequenza cardiaca registrata da dispositivi sanitari o di fitness). In linea di principio, l'espressione "forniti dall'interessato" deve essere

[40] Si segnala il parere 05/2014 del WP216 sulle tecniche di anonimizzazione (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_it.pdf). Qui il Gruppo di lavoro ha definito "dati anonimi" quei dati privati di elementi sufficienti per impedire l'identificazione della persona interessata, vale a dire che sono stati trattati in maniera tale da non poter essere più utilizzati per identificare una persona utilizzando «l'insieme dei mezzi che possono essere ragionevolmente utilizzati» dal responsabile del trattamento o da altri. Rimandando al parere per una trattazione completa, si specifica che esso ha fornito un contributo sulle tecniche di anonimizzazione, esaminandone l'efficacia e i limiti rispetto al quadro giuridico dell'UE in materia di protezione dei dati e fornendo raccomandazioni per il loro impiego, tenendo altresì conto del rischio residuo di identificazione insito in ciascuna di esse.
Tra le tecniche illustrate nel parere ci sono la "randomizzazione" e la "generalizzazione". La prima rappresenta una famiglia di tecniche – tra le quali troviamo la permutazione e la privacy differenziale – che modifica la veridicità dei dati al fine di eliminare la forte correlazione che esiste tra i dati e la persona; va da sé che se i dati sono sufficientemente incerti non possono più essere riferiti a una persona specifica. Di per sé la randomizzazione non riduce l'unicità di ogni dato, in quanto ciascun dato può comunque essere ancora estrapolato da un'unica persona interessata, ma può rappresentare una tutela dagli attacchi/rischi di deduzione e può essere affiancata da tecniche di generalizzazione per fornire maggiori garanzie di tutela della sfera privata.
La generalizzazione rappresenta la seconda famiglia di tecniche di anonimizzazione – la quale ricomprende l'aggregazione, il k-anonimato e la L-L-diversità/t-vicinanza – e consiste nel generalizzare, o "diluire", gli attributi delle persone interessate modificando la rispettiva scala o ordine di grandezza; significa, ad esempio, considerare una regione anziché una città oppure un mese anziché una settimana. Sebbene possa essere efficace per impedire l'individuazione, la generalizzazione non consente un'anonimizzazione che risulti efficace in tutti i casi; in particolare, presuppone approcci quantitativi specifici e sofisticati per impedire la correlabilità e la deduzione.
Il WP29 sottolinea come il conoscere i principali punti di forza e debolezza di ciascuna tecnica sia utile per decidere come progettare un processo di anonimizzazione adeguato in un determinato contesto.

interpretata in modo estensivo, escludendo unicamente i "dati inferenziali" e i "dati derivati"[41]. Ad esempio, l'esito della valutazione dello stato fisico di un utente derivante dall'analisi dei dati forniti attraverso un dispositivo fitness non può essere di per sé considerata come "fornita dall'interessato", anche se spesso fa parte del profilo di cui è in possesso il titolare, perché frutto di un'elaborazione, compita dal titolare, dei dati forniti dall'interessato. Ciò che questi può fare, però, è di esercitare il diritto di ottenere dal titolare del trattamento la conferma che sia, o meno, in corso un trattamento di dati personali che lo riguardano e in caso di risposta affermativa, di ottenerne l'accesso nonché di ottenere informazioni sull'esistenza di decisioni automatizzate, compresa la profilazione ex art. 22 e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché sull'importanza e le conseguenze previste da tale trattamento per l'interessato, sulla base del diritto di accesso riconosciuto dall'art. 15 del Regolamento.

4.5 Diritto di opposizione

Il diritto di opposizione, già conosciuto nel nostro ordinamento, è una delle conferme operate dal Regolamento (UE) 2016/679, il quale però lo "ripropone" presentandolo sotto una diversa luce: mentre prima era inteso in un senso puramente negativo – vale a dire come la facoltà di impedire l'intromissione di estranei nella propria vita privata o di rifiutare la diffusione di informazioni sul proprio conto – oggi, al contrario, ha acquisito una connotazione positiva, ossia come affermazione della libertà e della dignità della persona e come potere di controllare i mezzi con i qual vengono diffusi i propri dati e le finalità per le quali questi vengono trattati.

L'art. 21 del Regolamento (UE) 2016/679 attribuisce a questo diritto, oltre alla connotazione positiva appena evidenziata, anche una valenza autonoma, consentendo all'interessato di opporsi in qualsiasi momento, per motivi connessi alla sua condizione particolare al trattamento dei dati personali che lo riguardano; a tale opposizione corrisponde l'immediato obbligo, in capo al titolare, di astenersi dal trattare ulteriormente i dati, salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgano sugli interessi, sui diritti e sulle libertà dell'interessato[42] oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Analogo discorso può essere fatto con riferimento all'opposizione al trattamento di dati personali per finalità di marketing diretto: in questo caso, però, il corrispondente obbligo del titolare di cessare ogni forma di trattamento è assoluto, non potendo egli opporre l'esistenza di motivi legittimi e/o "giudiziari". Il diritto di opposizione, esercitabile per motivi connessi alla propria condizione particolare o per opporsi a finalità di marketing diretto, deve essere portato all'attenzione dell'interessato e presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato (art. 21 parag. 4).

[41] I dati inferenziali e i dati derivati sono quelli creati dal titolare sulla base dei dati forniti dall'interessato e comprendono anche i dati personali generati da un fornitore di servizi.

Da ultimo, l'interessato, sempre per motivi connessi alla propria condizione particolare, ha il diritto di opporsi qualora i propri dati siano trattati a fini di ricerca scientifica o storica o a fini statistici ai sensi dell'art. 89; in questo caso il titolare può invocare la necessità del trattamento per l'esecuzione di un compito di interesse pubblico.

4.6 Processo decisionale automatizzato

Nonostante un tale processo fosse già conosciuto ai titolari del trattamento dei dati personali, il legislatore europeo ha inteso inserirlo nel nuovo Regolamento, riconoscendo la potenziale pericolosità di un trattamento automatizzato di dati personali che può sfociare in decisioni che sono proprie della macchina e non dell'uomo; uno strumento, pertanto, per arginare il "sopravvento" della sterile tecnologia.

L'art. 22 ha riconosciuto, a riguardo, il diritto dell'interessato a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. Un tale diritto deve però essere contemperato con altre esigenze e pertanto non si applica, così come disposto dall'art. 22 parag. 2, nel caso in cui la decisione:

a) Sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento. In questo caso il titolare è tenuto ad adottare misure appropriate per tutelare i diritti, le libertà e gli interessi legittimi dell'interessato consentendogli almeno l'esercizio del diritto di ottenere l'intervento umano da parte del titolare, di esprimere la propria opinione e di contestare la decisione.

b) Sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;

c) Si basi sul consenso esplicito dell'interessato. Anche in tale ipotesi, come *supra* per il punto a), il titolare è tenuto all'adozione di misure appropriate e a consentire all'interessato l'esercizio di diritti minimi.

Il titolare del trattamento, inoltre, è tenuto a predisporre misure tecniche e organizzative per garantire – e all'occorrenza essere in grado di dimostrare – che il trattamento dei dati personali venga effettuato conformemente al Regolamento (c.d. principio di *accountability* per il quale si rimanda *supra* al cap. 4.3).

Il tema della **sicurezza** è regolato specificamente all'art. 32 del Regolamento (UE) 2016/679 e per la cui trattazione analitica si rimanda *infra* al cap 8.2.

4.7 Limitazioni all'esercizio dei diritti da parte degli interessati

Il legislatore europeo, all'art. 23, si preoccupa di regolare specificamente la possibilità che il diritto dell'Unione o degli Stati membri, cui sono soggetti il titolare e/o il responsabile del trattamento, possa limitare sia la portata degli obblighi e dei diritti fin qui elencati (artt. 12-22 e 34 del Regolamento). In primo

luogo, a tal fine, è necessario che le disposizioni limitative rispettino l'essenza dei diritti e delle libertà fondamentali e che le relative misure siano necessarie e proporzionate in una società democratica in modo da salvaguardare:

a) La sicurezza nazionale;

b) La difesa;

c) La sicurezza pubblica;

d) La prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;

e) Altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale;

f) La salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari;

g) Le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate;

h) Una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere a) - e) e g);

i) La tutela dell'interessato o dei diritti e delle libertà altrui;

j) L'esecuzione delle azioni civili.

In secondo luogo e in particolare, prosegue l'art. 23 parag. 2, qualsiasi misura di quelle appena elencate contiene disposizioni specifiche riguardanti almeno, se del caso:

a) Le finalità del trattamento o le categorie di trattamento;

b) Le categorie di dati personali;

c) La portata delle limitazioni introdotte;

d) Le garanzie per prevenire abusi o l'accesso o il trasferimento illeciti;

e) L'indicazione precisa del titolare del trattamento o delle categorie di titolari;

f) I periodi di conservazione e le garanzie applicabili tenuto conto della natura, dell'ambito di applicazione e delle finalità del trattamento o delle categorie di trattamento;

g) I rischi per i diritti e le libertà degli interessati;

h) Il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità della stessa.

5.I SOGGETTI DEL REGOLAMENTO

Alcuni dei soggetti che troviamo nel Regolamento (UE) 2016/679 sono già conosciuti (in modo sovrapponibile) al nostro ordinamento grazie al Codice per la protezione dei dati personali (D.lgs n. 196/2003), altre figure invece sono nuove ed altre ancora, seppur già conosciute, sono state parzialmente modificate. Il Regolamento infatti ha in parte rivisto l'originaria impostazione e le funzioni delle principali figure soggettive, introducendone anche altre; tali cambiamenti si sono resi necessari anche conseguentemente all'evoluzione dei concetti di privacy e protezione dei dati personali per assicurare la giusta tutela in seguito alla diffusione del processo tecnologico.

5.1 L'interessato

L'interessato è qualsiasi persona fisica identificata o identificabile, considerando per tali le persone fisiche che possono essere identificate, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. In altre parole l'interessato è colui al quale si riferiscono i dati personali, vale a dire qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

5.2 Il titolare del trattamento

Il titolare è «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, 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 n. 7) Regolamento).

Nell'ambito dell'organizzazione dell'ente o dell'azienda il titolare è una figura fondamentale ed è coincidente con il concetto a noi già noto grazie al Codice per la protezione dei dati personali. La sua rilevanza lo porta ad adottare politiche e ad attuare misure tali da garantire ed essere in grado di dimostrare che il trattamento dei dati effettuato sia conforme alla normativa, in virtù del principio di *accountability*. Queste misure consistono nella legittima conservazione della documentazione, nell'attuazione dei necessari requisiti di sicurezza dei dati, nell'esecuzione della valutazione d'impatto sulla protezione dei dati, nel rispetto dei requisiti di autorizzazione preventiva o di consultazione preventiva dell'autorità di controllo e del responsabile della protezione dei dati e nella definizione di informazioni e comunicazioni trasparenti da fornire all'interessato.

Sempre connesso alla figura del titolare del trattamento è il principio della *privacy by design*[43], per il quale egli – tenuto conto dell'evoluzione tecnica e dei costi di attuazione – deve mettere in atto adeguate misure e procedure tecniche e organizzative tali da rendere il trattamento conforme al Regolamento e assicurare la tutela dei diritti dell'interessato.

5.3 Il responsabile del trattamento

Il responsabile del trattamento, secondo la definizione fornita dall'art. 4 n. 8) del Regolamento, è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Il nuovo Regolamento dà alla figura del responsabile del trattamento una rilevanza tale che si può dire diventi quasi una figura professionale a sé. L'art. 28, proprio con riferimento alla figura del responsabile, dispone infatti che «qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate […]». La scelta pertanto non ricade su un soggetto (fisico o giuridico) qualsiasi, ma su chi è già in possesso di determinate e specifiche competenze, per cui è di tutta evidenza che anche il responsabile del trattamento debba avere una competenza specifica. Grazie al possesso di queste competenze specifiche il responsabile collabora concretamente con il titolare del trattamento per la creazione delle condizioni tecniche e organizzative necessarie per l'adempimento dell'obbligo – in capo a quest'ultimo – di dare seguito alle richieste per l'esercizio dei diritti dell'interessato, assumendo peraltro determinate responsabilità derivanti dalla stipula di un accordo contrattuale. Si parla di regolamento contrattuale in quanto l'esecuzione dei trattamenti su commissione deve essere disciplinata, a norma del regolamento, da un contratto o altro atto giuridico che vincoli il titolare del trattamento al responsabile e con cui si regolino la materia, la durata, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Conseguentemente anche lo stesso accordo tra titolare e responsabile del trattamento deve avere il suo fondamento giuridico in un contratto o in altro atto giuridico che preveda, altresì, una serie di obblighi in capo al responsabile del trattamento.

5.4 Il Data Protection Officer (DPO)

La figura del Data Protection Officer (o Responsabile Protezione Dati – RPD) o non è una novità assoluta; la sua nomina, infatti, era una pratica già in uso in vari Stati membri durante la vigenza della Direttiva n. 95/46/CE. La novità pertanto risiede non già nella semplice previsione della figura del RPD, bensì nella sua obbligatorietà.

[43] L'argomento è stato trattato *supra* al cap. 4.4

Gli articoli del Regolamento cui fare riferimento in tema di responsabile della protezione dei dati sono il 37, 38, 39: questi disciplinano con chiarezza le modalità di designazione del responsabile, la sua posizione e i compiti che esso è chiamato a svolgere.

Secondo quanto disposto dall'art. 37 parag. 1, la nomina del RPD effettuato dal titolare e dalla responsabile del trattamento ogniqualvolta questo venga effettuato da un'autorità pubblica o da un organismo pubblico (ad eccezione delle autorità giurisdizionali nell'esercizio delle loro funzioni giurisdizionali) ovvero qualora le principali attività del titolare o del responsabile del trattamento richiedono il monitoraggio regolare e sistematico degli interessati su "larga scala" oppure implichino il trattamento di dati idonei a rivelare l'origine razziale o etnica, le convinzioni religiose filosofiche, opinioni politiche, appartenenza sindacale ovvero il trattamento di informazioni consistenti in dati biometrici o genetici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale della persona o al suo orientamento sessuale o, infine, dati relativi a condanne penali o a reati di cui all'art. 10 del Regolamento (UE) 2016/679.

I casi di cui al paragrafo 1 sono tutte ipotesi di designazione obbligatoria del RPD. Il successivo paragrafo 4 introduce la possibilità secondo la quale, al di fuori delle ipotesi elencate al paragrafo 1, i titolari e i responsabili del trattamento o le associazioni e gli altri organismi di rappresentanza degli stessi, possano – ovvero debbano qualora l'obbligo sia imposto dal diritto interno di ciascuno Stato membro o dell'Unione in ulteriori ipotesi rispetto a quelle già esaminate – designare un RPD, il quale può agire per le associazioni e gli altri organismi che lo hanno nominato. Al di fuori quindi delle ipotesi di designazione specificamente previste dal Regolamento, le organizzazioni possono trovare conveniente nominare, spontaneamente, un RPD e anche il Gruppo dei Garanti europei (WP29) incoraggia tali nomine su base volontaria. È inoltre ben possibile che un'azienda o un ente, quando non sia soggetto all'obbligo di designare un RPD e non intenda procedere a tale designazione su base volontaria, ricorra comunque a personale o consulenti esterni incaricati di incombenze relative alla protezione dei dati personali. In tal caso però è fondamentale garantire che non vi siano ambiguità in termini di denominazione, status e compiti di queste figure; è dunque essenziale che in tutte le comunicazioni interne all'azienda e anche in quelle esterne – con l'autorità di controllo, gli interessati, i soggetti esterni in genere – queste figure o consulenti non siano indicati con la denominazione di RPD. Quanto appena considerato vale anche i Chief privacy Officer (CPO) o altri professionisti in materia di privacy già operati presso alcune aziende, che non sempre e non necessariamente si conformano ai requisiti fissati nel regolamento per quanto riguarda, ad esempio, le risorse disponibili o le salvaguardie della loro indipendenza e che, in tal caso, non possono essere considerati e denominati RPD.

Si rende necessaria, prima di procedere con l'esame della figura del RPD, aprire una breve parentesi circa alcuni termini appena utilizzati in tema di nomina obbligatoria, al fine di fornire – supplendo così alle mancanze del Regolamento – alcune definizioni. È possibile fare le precisazioni che seguono grazie anche al lavoro del Gruppo dei Garanti europei (WP29), il quale con un documento, facente parte di un gruppo di tre, oltre che ad aiutare gli Stati membri ad adeguare le proprie normative interne e a sensibilizzare le imprese alle novità introdotte dal nuovo Regolamento (UE), ci fornisce le delucidazioni di cui necessitiamo.

Per identificare nel concreto l'"autorità pubblica" o l'"organismo pubblico" si deve fare riferimento al diritto nazionale; di conseguenza, sono tali le autorità nazionali, regionali e locali ma, a seconda del diritto nazionale applicato, la nozione può ricomprendere anche tutta una serie di altri organismi di diritto pubblico. Come abbiamo appena visto, in questi casi la nomina del RPD è obbligatoria. Vi sono però altri soggetti

(persone fisiche e giuridiche) che possono validamente svolgere funzioni pubbliche ed esercitare pubblici poteri pur non essendo autorità pubbliche o organismi pubblici: si pensi ad esempio al settore dei trasporti pubblici, alle forniture idriche ed elettriche, alle infrastrutture stradali, alle emittenti radiotelevisive pubbliche, agli istituti per l'edilizia pubblica o agli organismi di disciplina professionale. Per questi soggetti, pur non sussistendo un obbligo formale di nomina del RPD, se ne consiglia comunque il ricorso, dal momento che anche nei confronti di questi soggetti il titolare ha un margine esiguo o nullo rispetto alla possibilità di decidere se e come possano essere trattati i propri dati personali, rendendosi verosimile la necessità dell'ulteriore tutela offerta dal RPD.

Per quanto riguarda, invece, le "attività principali" del titolare o del responsabile del trattamento si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi che questi soggetti perseguono. Nel Considerando 97 si afferma che le attività principali di un titolare del trattamento «riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria». Tale espressione non deve essere interpretata però nel senso di escludere quei casi in cui il trattamento dei dati costituisce una componente inscindibile delle attività svolte dal titolare o dal responsabile del trattamento. Ad esempio, un'impresa di sicurezza privata incaricata della sorveglianza di più centri commerciali e aree pubbliche svolge come attività principale proprio la sorveglianza, ma questa, a sua volta, è legata in modo inscindibile al trattamento dei dati personali. Ne consegue che l'impresa sarà soggetta all'obbligo di nominare un RPD. Diverso invece è il caso del pagamento delle retribuzioni. È certamente una funzione di supporto necessaria ai fini dell'attività principale o dell'oggetto principale del singolo organismo, ma pur essendo necessaria o essenziale è solitamente considerata accessoria e non viene annoverata tra le attività principali che portano un obbligo di nomina del RPD.

Per quanto riguarda il trattamento su "larga scala", siamo sprovvisti, anche in questo caso, di una definizione legislativa in quanto il regolamento non ne fornisce. Anche in questo caso bisogna rifarsi alle Linee guida del WP29. Queste, se lette unitamente al Considerando 91 del Regolamento (UE) 2016/679, costituiscono un valido aiuto per verificare se si è o meno alla presenza di un simile trattamento. A tal fine devono essere considerati i seguenti fattori:

- √ Il numero di persone interessate, intese come numero specifico ovvero come percentuale della popolazione in questione;
- √ Il volume dei dati e/o la gamma di differenti unità di dati da elaborare;
- √ La durata o la permanenza dell'attività di elaborazione dei dati;
- √ L'estensione geografica dell'attività di trasformazione.

Sulla base di questi fattori possiamo considerare come trattamento su larga scala quello dei dati di profilazione per la pubblicità di un motore di ricerca o quello dei dati (contenuti, traffico, posizione) da parte dei fornitori di servizi telefonici o internet. Al contrario, non costituiscono una tale elaborazione il trattamento dei dati dei pazienti da parte di un singolo medico o quello effettuato da un singolo avvocato con riferimento ai dati personali relativi a condanne penali e reati.

Da ultimo, per definire "monitoraggio regolare e sistematico" dobbiamo ancora una volta fare affidamento al lavoro del WP29 e al Considerando 24. Quest'ultimo vi ricomprende tutte le forme di tracciamento e profilazione su internet anche per finalità di pubblicità comportamentale: si legge infatti che «per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportanti e le posizioni personali». Il Gruppo dei Garanti europei si sofferma anche sul significato di "regolare" e "sistematico". Il primo, a giudizio del WP29, ha almeno uno dei seguenti significati:

- √ Che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
- √ Che è ricorrente o che viene ripetuto a intervalli costanti;
- √ Che avviene in modo costante o a intervalli periodici.
- √ Per il termine "sistematico", invece, possono essere considerati i seguenti significati:
- √ Che avviene per sistema;
- √ Predeterminato, organizzato o metodico;
- √ Che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- √ Svolto nell'ambito di una strategia;

Si possono fare alcune esempi di attività che possono configurare un monitoraggio regolare e sistematico di interessati, in modo da rendere più chiari le nozioni appena espresse: il reindirizzamento di messaggi di posta elettronica, le attività di marketing basate sull'analisi dei dati raccolti; la profilazione e lo *scoring* per finalità di valutazione del rischio; l'utilizzo di telecamere a circuito chiuso o di dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica e in generale tutti quei dispositivi definiti smart.

Tornando ad esaminare la figura del RPD, la sua nomina potrà essere effettuata, dal titolare o dal responsabile del trattamento, scegliendo la figura tra i propri dipendenti (RPD-dipendente) o affidando l'incarico a un terzo sulla base di un contratto di servizi (RPD-esterno).

Inoltre, è facoltà di un gruppo imprenditoriale nominare un unico responsabile della protezione dei dati, a condizione che questi sia facilmente raggiungibile da ogni stabilimento. Tale concetto viene riferito ai compiti del RPD quale punto di contatto per i soggetti titolari dei dati trattati, dell'autorità di vigilanza, ma anche per il personale interno dell'organizzazione. Pertanto il RPD dovrà essere in grado di comunicare e cooperare efficientemente con tutti questi soggetti, utilizzando anche la lingua (o le lingue) dell'autorità di vigilanza o delle persone interessate. La disponibilità personale del RPD – sia fisicamente all'interno dei locali aziendali nel caso di RPD-dipendente ovvero attraverso un numero verde o un altro mezzo di comunicazione sicuro – è indispensabile per garantire agli interessati il diritto a contattarlo. A tale riguardo l'art. 37 parag. 7 del Regolamento prevede l'obbligo, a carico del titolare del trattamento o del responsabile

del trattamento, di pubblicare i dati di contatto (indirizzo postale, numero di telefono o casella e-mail dedicati) del responsabile della protezione dei dati e di comunicarli conseguentemente all'autorità di controllo. Si ricorda – rimandando agli artt. 51-59 del Regolamento per maggiore completezza – che l'autorità di controllo è quell'organismo indipendente incaricato di sorvegliare l'applicazione del Regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali e di agevolare la libera circolazione dei dati personali all'interno dell'Unione. Per esemplificare, tale figura è per noi rappresentata dal Garante per la protezione dei dati personali. In questo modo tanto gli interessati (interni ed esterni all'organizzazione) quanto le autorità di vigilanza possono facilmente, direttamente e in forma riservata contattare il RPD senza doversi necessariamente rivolgere a un'altra struttura operante presso il titolare o il responsabile del trattamento.

Non necessariamente il nome del RPD deve essere "in chiaro", anche se la sua pubblicazione potrebbe essere una buona pratica da attuare in determinate circostanze. Sul punto si fa notare come l'art. 33 parag. 3 lett. b), nel descrivere le informazioni che devono essere fornite all'autorità di vigilanza e alle persone interessate in caso di violazione dei dati personali – diversamente dall'art. 37 parag. 7 – richiede in particolare che venga comunicato anche il nome (e non solo i dettagli di contatto) del RPD. Seppure la comunicazione del nominativo non risulti necessaria ai sensi del Regolamento, rappresenta con ogni probabilità una buona pratica e spetta al titolare, al responsabile del trattamento e allo stesso RPD stabilire se si tratti di un'informazione necessaria o utile nelle specifiche circostanze. Tuttavia, si precisa come la comunicazione del nominativo del RPD all'autorità di controllo sia fondamentale affinché il RPD possa fungere da punto di contatto tra l'ente/organismo e l'autorità di controllo stessa.

Al di là della scelta operata è necessario che il RPD possa adempiere alle proprie funzioni e ai propri compiti in maniera indipendente e, pare ovvio dirlo, rispettando tutti i requisiti stabiliti negli artt. 37-39 del Regolamento. Ad esempio il RPD non dovrà trovarsi in conflitto di interessi con il titolare del trattamento, tanto esternamente quanto internamente all'organizzazione. Per questo motivo qualora il RPD fosse autorizzato a svolgere altre funzioni, in accordo con quanto disposto dall'art. 38 parag. 6, è necessario che queste non gli consentano di determinare le finalità e gli strumenti del trattamento dei dati personali, in modo tale che egli possa mantenere la propria autonomia e indipendenza.

Al fine di rendere applicabile quanto disposto dal Regolamento in tema di conflitto di interessi – o meglio, al fine di evitare il verificarsi di un conflitto – il Gruppo dei Garanti europei, nel medesimo documento sopra citato, ha indicato una serie di buone prassi – modificabili sulla base della struttura organizzativa specifica di ogni organizzazione – che il titolare e il responsabile possono adottare. Sarebbe, pertanto, consigliabile:

- √ Individuare le posizioni che sarebbero incompatibili con le posizioni di RPD;
- √ Elaborare un regolamento interno che eviti la formazione di conflitti di interesse, dandone contemporaneamente una definizione più generale;
- √ Dichiarare che il proprio RPD non ha alcun conflitto di interesse con riferimento alla propria funzione, per una maggiore sensibilizzazione sul tema.

Ferma la libertà di scelta e sempre nel rispetto delle disposizioni del Regolamento, ciò che dovrebbe guidare il titolare o il responsabile del trattamento nella designazione del RPD è il grado di conoscenze specialistiche che questi detiene; il livello di competenza richiesto, infatti, non è strettamente definito ma deve essere commisurato con la sensibilità, la complessità e la quantità di dati trattati nell'ambito di ciascun processo organizzativo. Logica conseguenza è che nel caso in cui un'attività di trattamento risulti particolarmente complessa ovvero comporti una grande quantità di dati sensibili, il livello di competenza del RPD dovrebbe essere più elevato. Sul punto, il Gruppo dei Garanti europei supplisce ancora una volta alle mancanze del Regolamento (UE) 2016/679 e identifica, a scopo puramente esemplificativo e non esaustivo, alcune qualità professionali del RPD che dovrebbero essere considerate al momento della sua scelta:

- √ Conoscenza approfondita delle leggi e delle pratiche (nazionali ed europee) sulla protezione dei dati personali nonché del Regolamento (UE) 2016/679;
- √ Conoscenze del settore in cui l'impresa opera e dell'organizzazione del titolare del trattamento;
- √ Sufficiente conoscenza dei processi operativi applicati e delle esigenze di sicurezza e protezione dei dati del titolare.

Anche il Garante italiano si è occupato dei criteri di scelta del Responsabile della protezione dei dati e l'ha fatto pubblicando una nota (del 20.07.2017 inviata all'Azienda Ospedaliera dei Colli) dalla quale si evince la necessità di competenze specifiche in materia piuttosto che di attestati formali. Certo questi ultimi, quale esito della partecipazione ad attività specialistiche (ad esempio master, corsi di studio e professionali) sono apprezzabili, soprattutto per attestare la conoscenza del nuovo Regolamento, ma le competenze specifiche in materia, acquisite con una documentata esperienza professionale sono preferibili.

Il Garante italiano sottolinea poi come le disposizioni non prevedano un albo dei responsabili della protezione dei dati che attesti i requisiti e le caratteristiche di conoscenza, abilità e competenza previste dal nuovo Regolamento e nemmeno richiedono che tali requisiti siano attestati attraverso specifiche certificazioni.

Per supplire a questa mancanza di "formalità" si potrebbe ricorrere – così come sta succedendo per altre "professioni non regolamentate" – alla certificazione volontaria delle competenze professionali effettuata da appositi enti certificatori. Queste certificazioni – che non rientrano tra quelle disciplinate dall'art. 42 del Regolamento, come specificato dal Garante italiano – rilasciate anche all'esito della partecipazione ad attività formative e alla verifica dell'apprendimento, non equivalgono di per sé a un'abilitazione allo svolgimento del ruolo di RPD, anche se possono rappresentare un ottimo strumento per valutare il possesso di un livello minimo di conoscenza della disciplina.

Queste sono alcune delle competenze professionali del RPD esemplificate dai Garanti italiano ed europeo; quest'ultimo, peraltro, si è preoccupato di fare riferimento anche ad alcune sue qualità personali, quali l'integrità morale e l'etica professionale. I RPD infatti svolge un ruolo chiave nella promozione di una cultura della protezione dei dati all'interno dell'azienda, aiutando a implementare quegli elementi essenziali del Regolamento, quali: i principi di elaborazione dei dati, i diritti delle persone interessate, la protezione dei dati di progettazione e di default, i registri delle attività di trattamento, la notifica e la comunicazione della

violazione dei dati. Secondo il Gruppo dei Garanti la sua preoccupazione primaria dovrebbe essere quella di garantire la conformità delle procedure di trattamento con il Regolamento, adempiendo ai propri compiti in conformità al diritto dell'Unione e degli Stati membri, rispettando il segreto e la riservatezza (art. 38 parag. 5 Regolamento): questi rivestono infatti una certa importanza in quanto i dipendenti potrebbero essere riluttanti a presentare reclami al RPD qualora non fosse assicurata la confidenzialità delle loro comunicazioni.

Si ricorda, a proposito, che il RPD non è personalmente responsabile della mancata conformità tra trattamento effettuato e disposizioni del Regolamento (UE) 2016/679; questo infatti è compito del titolare del trattamento (controller) e del responsabile del trattamento (processor) i quali devono poter dimostrare che il trattamento è effettuato in osservanza con quanto prescritto dal Regolamento. Si approfitta per fare un breve appunto terminologico non certo di scarsa rilevanza. I più attenti avranno notato che le figure del controller e del processor non corrispondono a quelle conosciute fino a questo momento: infatti, durante la vigenza della Direttiva 95/46/CE il primo corrispondeva al nostro responsabile del trattamento, mentre il secondo all'incaricato. I riferimenti sono cambiati in seguito all'entrata in vigore del Regolamento (UE) 2016/679 e sono specificamente legati alla sua traduzione italiana, proposta dal nostro Garante per la protezione dei dati personali alla Commissione e da questa accettata. La ragione di una tale traduzione risiede probabilmente nella necessità di evitare complicazioni interpretative e adeguare il nuovo Regolamento alle figure di carattere decisionale nell'ambito della privacy già note nel nostro ordinamento. Ciò che pertanto ora viene a mancare, nel Regolamento, è la figura dell'incaricato così come da noi conosciuto nel D.lgs n. 196/2003, ma del resto nella Direttiva 95/46/CE vi era l'assenza della figura del nostro titolare del trattamento.

Secondo l'art. 38 parag. 1 il RPD dovrà essere «tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali». È fondamentale, pertanto, che il RPD sia informato e consultato preventivamente, in modo tale da facilitare il rispetto del Regolamento e assicurare un adeguato livello di privacy. Il WP29 si raccomanda, a tal proposito, di:

- √ Permettere la presenza del RPD in tutte quelle sedi in cui vengono prese decisioni che potrebbero ripercuotersi sulla protezione dei dati;
- √ Trasmettergli tempestivamente tutte le informazioni pertinenti al suo ruolo in modo tale che egli possa fornire una consulenza adeguata;
- √ Dare il giusto peso al suo parere e, in caso di disaccordo, di documentare in modo puntuale le ragioni per le quali si è deciso di discostarsi dalla linea del RPD.

Il paragrafo 2 dell'art. 38 prevede il supporto del RPD da parte del titolare e del responsabile del trattamento nell'esecuzione dei suoi compiti, fornendogli le risorse necessarie per assolverli e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica. In linea di principio, quanto più aumentano la complessità e/o la sensibilità dei trattamenti, tanto maggiori dovranno essere le risorse messe a disposizione del RPD; la divisione "protezione dati" – se così vogliamo chiamarla – deve infatti poter operare con efficienza potendo contare su risorse sufficienti in proporzione al trattamento svolto. Questo obbligo di sostegno si sostanzia in una serie di elementi:

- √ Sostegno attivo del RPD da parte del management;

- √ Tempo sufficiente per adempiere ai propri doveri: ciò è di primaria importanza qualora il RPD svolga le sue funzioni part-time ovvero in aggiunta ad altri compiti, vale a dire qualora le sue funzioni non siano svolte in modo esclusivo e a tempo pieno;
- √ Sostegno adeguato in termini di risorse finanziarie, infrastrutture (locali, attrezzature, strutture) e di personale, se necessario;
- √ Comunicazione ufficiale, a tutto il personale, della designazione del RPD al fine di garantire che la sua esistenza e funzione sia conosciuta all'interno dell'organizzazione;
- √ Accesso ad altri settori aziendali, quali ad esempio le risorse umane, l'area legale, l'Information Technology, la sicurezza, in modo che il RPD possa ricevere il supporto necessario oltre che le informazioni in possesso delle altre aree aziendali;
- √ Un'adeguata formazione continua, dando la possibilità al RPD di rimanere aggiornato e di aumentare costantemente il proprio livello di competenza, incoraggiandolo a partecipare a corsi di formazione sulla protezione dei dati e ad altre forme di sviluppo professionale (partecipazione a forum, workshop, ecc.);

In caso di organizzazioni di grandi dimensioni o particolarmente strutturate potrebbe risultare conveniente affiancare dei collaboratori al RPD: in questo caso è fondamentale mettere per iscritto la struttura interna del team formato dal RPD e dal suo personale, nonché i compiti e le responsabilità di ciascun componente. Discorso speculare può essere fatto nel caso di RPD-esterno, il quale potrà servirsi, sotto la sua supervisione e responsabilità, di collaboratori per meglio svolgere i compiti assegnatigli.

Il Regolamento (UE) 2016/679 si preoccupa, come logico, di elencare anche i compiti cui il RPD è chiamato e lo fa prevedendone un minimo, lasciando agli Stati membri la possibilità di prevederne altri. Le funzioni del RPD sono raccolte nell'art. 39:

- **a)** Informare e fornire consulenza al titolare o al responsabile del trattamento nonché ai dipendenti che lo eseguono, in merito agli obblighi derivanti dal Regolamento nonché da altre disposizioni dell'Unione e degli Stati membri relative alla protezione dei dati;
- **b)** Sorvegliare l'osservanza del Regolamento e di tutte le altre disposizioni (europee e nazionali) relative alla protezione dei dati. In particolare, dovrà procedere alla raccolta di informazioni per individuare i trattamenti svolti, analizzare e verificare che i trattamenti siano conformi alle disposizioni di legge, svolgere attività di informazione, consulenza e indirizzo nei confronti del titolare o del responsabile del trattamento. Inoltre dovrà sorvegliare le politiche del titolare o del responsabile del trattamento in materia, comprese l'attribuzione di responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo. È proprio in virtù di tale attribuzione che trova significato l'obbligo per il RPD di astenersi dallo svolgere altre funzioni che gli consentono di determinare le finalità e gli strumenti del trattamento dei dati personali, pena l'insorgere di un potenziale conflitto di interessi. Si tratta ovviamente di un elemento da valutare caso per caso, anche e soprattutto in relazione alla specifica struttura organizzativa del singolo titolare o responsabile del trattamento. In linea di massima si può affermare però che situazioni di conflitto sono possibili con riferimento a ruoli

manageriali di vertice quali quello di un amministratore delegato, di un responsabile finanziario o di un responsabile operativo, di un direttore risorse umane o di uno della divisione marketing o ancora del responsabile dell'Information Technology. In aggiunta, non è da escludere un potenziale conflitto anche in riferimento a posizioni che non sono di vertice, ma che comportano ugualmente la determinazione di finalità o mezzi del trattamento. Si ricorda ancora una volta come il controllo del rispetto del Regolamento non significhi che il RPD sia personalmente responsabile in casi di inosservanza. Il Regolamento evidenzia come spetti al titolare – e non al RPD – «mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al […] regolamento»;

c) Fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'art. 35 del Regolamento. Si rimanda al relativo articolo per una conoscenza più approfondita dello strumento, ma si ricorda che la valutazione dell'impatto sulla protezione dei dati personali da parte dei trattamenti che il titolare intende effettuare è necessaria qualora il trattamento preveda l'uso di nuove tecnologie e, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Il Gruppo dei Garanti europei si raccomanda, a tale proposito, che il titolare del trattamento si consulti con il RPD sulle seguenti tematiche: se condurre o meno una valutazione di impatto sulla protezione dei dati (DPIA secondo l'acronimo inglese), su quale metodologia adottare nel condurre una tale valutazione, se condurla con le risorse interne ovvero esternalizzandola, quali salvaguardie applicare, comprese le misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate e, da ultimo, se la valutazione sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al Regolamento.

d) Cooperare con l'autorità di controllo e fungere da suo punto di contatto per questioni connesse al trattamento, tra cui la consultazione preventiva ex art. 36, oltre a effettuare, se del caso, consultazioni relativamente a qualunque altra questione. Questi compiti attengono al ruolo di "facilitatore" attribuito al RPD: egli infatti 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 che le vengono attribuiti dall'art. 57 del Regolamento nonché ai fini dell'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi ex art. 58.

e) Considerare debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. Ciò significa che il RPD debba definire un ordine di priorità nell'attività svolta e si concentri sulle questioni che presentino maggiori rischi in termini di protezione dei dati. Di converso, non significa che il RPD debba trascurare di sorvegliare il grado di conformità di altri trattamenti associati a un livello di rischio comparativamente inferiore, anche se è indubbio che la disposizione chieda di dedicare un'attenzione prioritaria agli ambiti che presentino rischi più elevati.

Da ultimo si ritiene utile fare una piccola nota, sempre in tema di compiti del RPD, con riferimento alla tenuta del registro delle attività di trattamento. Nonostante l'art. 30 del Regolamento preveda che siano il

titolare o il responsabile del trattamento (e non il RPD) a tenere «un registro delle attività di trattamento svolte sotto la propria responsabilità ovvero un registro di tutte le categorie di trattamento svolte per conto di un titolare del trattamento», nella pratica spesso se ne occupano i RPD. Essi infatti realizzano l'inventario dei trattamenti e ne tengono un registro sulla base delle informazioni fornite loro dai vari uffici o unità che trattano dati personali. Va inoltre considerato il fatto che l'art. 39 parag. 1 del Regolamento contiene un elenco non esaustivo dei compiti del RPD e che pertanto nulla vieta al titolare o al responsabile del trattamento di affidargli anche quello di tenere il registro delle attività di trattamento sotto la responsabilità – è bene sottolinearlo – degli stessi titolare o responsabile del trattamento in quanto teoricamente compito loro.

6.L'INCARICATO

L'incaricato è colui il quale è autorizzato a compiere operazioni di trattamento dal titolare o dal responsabile. Nonostante la figura non sia espressamente prevista dal Regolamento, contrariamente al D.lgs n. 196/2003[44], non ne viene esclusa del tutto la presenza; infatti all'art. 4 parag. 1 n. 10) il legislatore europeo identifica la figura del "terzo" come «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.».

6.1 Autorità di Controllo

L'autorità di controllo è, secondo la definizione di cui all'art. 4 n. 21), «l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'art. 51». Questo sancisce l'obbligo per gli Stati membri di incaricare una o più autorità pubbliche indipendenti di sorvegliare l'applicazione del Regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche (con riguardo al trattamento) e di agevolare la libera circolazione dei dati personali all'interno dell'Unione. Sempre al fine di assicurare una coerente applicazione del Regolamento in tutta l'Unione, le diverse autorità di controllo cooperano tra loro e con la Commissione mediante il meccanismo di coerenza di cui agli artt. 63 e ss.. Qualora uno Stato scelga di nominare più autorità di controllo, dovrà designarne una che le rappresenti nel Comitato europeo per la protezione dei dati, per la cui trattazione si rimanda al cap. 6.7.

Nello svolgimento dei propri compiti l'autorità di controllo deve agire in piena indipendenza così come, allo stesso modo, esercita i poteri che le sono conferiti. Questo comporta che i membri di ogni autorità non subiscono pressioni esterne – dirette o indirette – e non sono soggetti a istruzioni né tantomeno le sollecitano. A ulteriore garanzia di indipendenza i membri dell'autorità[45], per tutta la durata del mandato, si astengono dal compiere qualunque azione incompatibile con le loro funzioni e non possono esercitare altra attività (incompatibile), remunerata o meno.

Ciascuna autorità di controllo, si legge nel Considerando 120, dovrebbe disporre delle risorse umane e finanziarie[46] necessarie per l'effettivo adempimento dei propri compiti, compresi quelli di assistenza reciproca e cooperazione con altre autorità di controllo in tutta l'Unione.

---

[44] L'art. 30 del Codice della Privacy, rubricato appunto "Incaricati del trattamento", nel prevedere tale figura dispone che «Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.». Continua al comma 2 specificando che «La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.».

[45] I membri dell'autorità sono nominati, attraverso una procedura trasparente, dai Parlamenti, Governi, Capi di Stato di ciascun Stato membro, oppure da un organismo indipendente incaricato della nomina a norma del diritto dello Stato membro.

[46] Le risorse finanziarie – per le quali l'autorità di controllo può essere assoggettata a meccanismi di controllo e/o monitoraggio – dovrebbero essere stanziate attraverso la predisposizione di un bilancio annuale, separato e pubblico, che può far parte del bilancio generale statale o nazionale (Considerando 120).

La competenza, i compiti e i poteri dell'autorità di controllo sono disciplinati dagli artt. 55-58 del Regolamento, ai quali si rimanda.

6.2 Autorità di controllo capofila

L'autorità di controllo capofila è l'autorità cui spetta in prima battuta la gestione di un trattamento transfrontaliero.

L'autorità di controllo capofila è l'autorità con la responsabilità primaria nell'affrontare un'attività di elaborazione dati transfrontaliera. Il trattamento transfrontaliero viene definito dall'art. 4 n. 23) come quel trattamento che ha luogo:

a) nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure

b) nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

Ciò significa che se un'organizzazione ha stabilimenti in Italia e in Francia e il trattamento dei dati personali si svolge nel contesto delle loro attività (vale a dire sia in Italia che in Francia), allora questo sarà considerato un trattamento transfrontaliero. Alternativamente, l'organizzazione potrà svolgere l'attività di trasformazione nel contesto del proprio stabilimento in Italia, ma se questa attività influisce sostanzialmente – o rischia di incidere in maniera sostanziale – sugli interessati sia in Italia che in Francia, allora anche in questo caso il trattamento sarà considerato come transfrontaliero.

Il Gruppo dei garanti si sofferma poi sul significato di "incide sostanzialmente" – non specificato dal Regolamento – chiarendo che l'autorità di vigilanza dovrà valutare ogni singolo caso, secondo il criterio del "più probabile che non". Nel fare questo dovrà tener conto del contesto del trattamento, della tipologia di dati, dello scopo del trattamento. Dovrà altresì valutare se il trattamento:

√ causi, o possa causare, danni, perdite o disagio agli individui;

√ limiti i diritti degli interessati o neghi loro un'opportunità;

√ influenzi, o rischi di compromettere la salute degli individui, il loro benessere, la loro serenità o la loro situazione finanziaria o economica;

√ apra scenari di discriminazione o trattamento sleale.

I criteri di individuazione dell'autorità di controllo capofila sono stabiliti dal combinato disposto degli artt. 55-56 del Regolamento: «Fatto salvo l'art. 55, l'autorità di controllo dello stabilimento principale o dello

stabilimento unico del titolare e del trattamento o responsabile del trattamento è competente ad agire in qualità di autorità di controllo capofila per i trattamenti transfrontalieri effettuati dal suddetto titolare del trattamento o responsabile del trattamento, secondo la procedura di cui all'articolo 60. […]».

Il concetto di stabilimento principale è definito dall'art. 4 co. 16 e differisce a seconda che si consideri la figura del titolare o del responsabile del trattamento:

a) con riguardo al titolare del trattamento con stabilimenti in più di uno Stato membro è il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale.

b) con riguardo, invece, al responsabile del trattamento con stabilimenti in più di uno Stato membro è il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del Regolamento.

Al fine di stabile dove si trovi lo stabilimento principale è anzitutto necessario individuare l'amministrazione centrale del titolare nell'Unione europea – se presente –, intesa come il luogo dove vengono prese le decisioni circa le finalità e gli strumenti del trattamento dei dati personali. Questo nel pieno rispetto del principio secondo cui la supervisione del trattamento transfrontaliero deve essere guidata da una sola autorità di controllo nell'Unione europea. La corretta identificazione dello stabilimento principale è nell'interesse tanto dal titolare quanto del responsabile del trattamento, perché fornisce loro la chiarezza sull'identità dell'autorità di vigilanza con la quale rapportarsi e che dovrà valutare la conformità del loro operato con il Regolamento.

In caso di gruppi di imprese con sede nell'Unione europea i criteri di individuazione sono i medesimi: la capogruppo dovrebbe essere considerata come stabilimento principale, a meno che le finalità e i mezzi del trattamento non siano determinati da un altro stabilimento.

Il Gruppo dei garanti ha predisposto un documento, allegato alle Linee guida in tema di autorità di controllo e costituito da semplici domande e risposte, che aiuta l'impresa nell'identificazione dell'autorità di controllo capofila con la quale relazionarsi.

Si rileva che, secondo quanto enunciato nel Considerando 127 del Regolamento, è possibile in casi specifici procedere a un controllo locale. Infatti, ogni autorità di controllo che non agisce in qualità di autorità di controllo capofila dovrebbe essere competente a trattare casi locali qualora il titolare o il responsabile del trattamento sia stabilito in più di uno Stato membro, ma l'oggetto dello specifico trattamento riguardi unicamente quello effettuato in un singolo Stato membro e coinvolga soltanto interessati in tale singolo Stato (ad esempio quando l'oggetto riguardi il trattamento di dati personali di dipendenti nell'ambito di specifici rapporti di lavoro in uno Stato membro). In tali casi, l'autorità di controllo dovrebbe informare senza indugio

l'autorità di controllo capofila sulla questione. Dopo essere stata informata, la capofila dovrebbe decidere se intende trattare il caso a norma della disposizione sulla cooperazione tra l'autorità di controllo capofila e altre autorità di controllo interessate ("meccanismo dello sportello unico"), ovvero se l'autorità di controllo che l'ha informata debba trattarlo a livello locale. Al momento della decisione, l'autorità di controllo capofila dovrebbe tenere conto dell'eventuale esistenza, nello Stato membro dell'autorità di controllo che l'ha informata, di uno stabilimento del titolare del trattamento o del responsabile del trattamento, al fine di garantire l'effettiva applicazione di una decisione nei confronti del titolare o del responsabile del trattamento. Qualora l'autorità di controllo capofila decida di trattare il caso, l'autorità di controllo che l'ha informata dovrebbe avere la possibilità di presentare un progetto di decisione, che l'autorità di controllo capofila dovrebbe tenere nella massima considerazione nella preparazione del proprio progetto di decisione nell'ambito di tale meccanismo di sportello unico.

Da ultimo si ricorda che «Le norme sull'autorità di controllo capofila e sul meccanismo di sportello unico non dovrebbero applicarsi quando il trattamento è effettuato da autorità pubbliche o da organismi privati nell'interesse pubblico. In tali casi l'unica autorità di controllo competente a esercitare i poteri a essa conferiti a norma del presente regolamento dovrebbe essere l'autorità di controllo dello Stato membro in cui l'autorità pubblica o l'organismo privato sono stabiliti» (Considerando 128).

6.3 Il Comitato europeo per la protezione dei dati

Il Comitato europeo per la protezione dei dati è disciplinato dagli artt. 68-76 del Regolamento e, per specifica previsione, è istituito come organismo dell'Unione dotato di personalità giuridica. Il Comitato è composto dalla figura di vertice di un'autorità di controllo per ciascuno Stato membro e dal Garante europeo per la protezione dei dati, o dai rispettivi rappresentanti e nel caso in cui uno Stato membro abbia nominato due o più autorità di controllo, nel Comitato siederà il rappresentante comune di tali autorità nominato conformemente al diritto dello Stato membro.

Alle attività e alle riunioni del Comitato ha diritto di partecipare la Commissione la quale, a tal fine, designa un proprio rappresentante. Il Presidente del Comitato[47] – il quale lo rappresenta nei rapporti esterni – comunica alla Commissione le attività[48].

Il Comitato svolge i suoi compiti – elencati all'art. 70 – con indipendenza e allo stesso modo esercita i poteri che gli sono conferiti nel Regolamento. Il suo regolamento interno – con il quale esso stabilisce le modalità del proprio funzionamento – è adottato dai due terzi dei suoi membri, mentre le deliberazioni vengono prese a maggioranza semplice dei suoi membri; se il Comitato europeo lo ritiene necessario, le sue deliberazioni hanno carattere riservato secondo le previsioni del proprio regolamento interno.

[47] Il Presidente, insieme a due Vice presidenti, è nominato dal Comitato tra i suoi membri, salvo se diversamente previsto dal Regolamento (UE) 2016/679.

[48] Inoltre il Presidente ha il compito di convocare le riunioni del Comitato e stabilirne l'ordine del giorno, notificare le decisioni adottate dal Comitato all'autorità di controllo capofila e alle autorità di controllo interessate e assicurare l'esecuzione tempestiva dei compiti del Comitato, in particolare in relazione al meccanismo di coerenza ex art. 63.Tutti questi compiti possono essere ripartiti tra il Presidente e i Vice presidenti attraverso il regolamento interno del Comitato (art. 74).

È inoltre possibile l'accesso – secondo le modalità previste dal Regolamento (CE) n. 1049/2001 – ai documenti trasmessi ai membri del Comitato, agli esperti e ai rappresentanti di terzi. Rimandando al testo integrale del Regolamento appena citato per una trattazione esaustiva sull'argomento, si vuole offrire in questa sede una sintetica panoramica sul diritto di accesso ai documenti delle Istituzioni UE. L'obiettivo del Regolamento è rendere più semplice l'accesso ai documenti delle istituzioni europee, prevedendo che i cittadini possano ricevere qualsiasi tipo di documento, alle condizioni previste dal Regolamento e nei limiti delle eccezioni previste. Il regolamento si applica a tutti i documenti detenuti da un'istituzione, vale a dire da essa prodotti oppure ricevuti e in suo possesso, in tutti i settori di attività dell'Unione europea. Può beneficiare del regolamento qualsiasi cittadino dell'Unione e qualsiasi persona fisica o giuridica che risieda o abbia la sede sociale in un paese dell'UE.

Vi sono però delle eccezioni per le quali le Istituzioni rifiutano l'accesso a un documento la cui divulgazione arrechi pregiudizio alla tutela di quanto segue:

- √ L'interesse pubblico, per quanto riguarda la sicurezza pubblica, la difesa, le relazioni internazionali, la politica finanziaria, monetaria o economica della Comunità o di un paese dell'UE;
- √ La vita privata e l'integrità di un individuo, in particolare in conformità con la legislazione comunitaria sulla protezione dei dati personali;
- √ Gli interessi commerciali di una persona fisica o giuridica;
- √ Le procedure giurisdizionali e la consulenza legale;
- √ Gli obiettivi delle attività ispettive, di indagine e di revisione contabile.

Inoltre, l'Istituzione può rifiutare l'accesso a un documento interno redatto da essa redatto qualora sussista il rischio che la sua divulgazione possa pregiudicare seriamente quel processo decisionale dell'istituzione, a meno che vi sia un interesse pubblico prevalente alla sua divulgazione.

Per quanto concerne i documenti di terzi, invece, l'istituzione consulta il terzo al fine di valutare se sia possibile applicare un'eccezione.

Qualora un Paese dell'UE riceva una domanda di accesso a un documento in suo possesso, che provenga da un'Istituzione, i due soggetti si consultano per assicurarsi che la divulgazione sia in linea con gli obiettivi del presente regolamento. In alternativa, il Paese dell'UE può deferire all'Istituzione la domanda di accesso. Questa è presentata in forma scritta, anche elettronica, in una delle lingue dell'UE e il richiedente non è tenuto a motivarla. La domanda di accesso ai documenti è trattata prontamente: al richiedente viene inviato un avviso di ricevimento ed entro quindici giorni lavorativi dalla registrazione della domanda, l'Istituzione formula una risposta positiva o negativa in merito all'accesso al documento richiesto. Nel caso di un rifiuto totale o parziale, il richiedente può, entro quindici giorni lavorativi dalla ricezione della risposta, chiedere alla stessa di rivedere la sua posizione, presentando una domanda di conferma. L'accesso ai documenti avviene mediante consultazione sul posto oppure tramite rilascio di una copia.

Per quanto riguarda l'accesso a documenti delicati[49] le relative domande sono trattate solo da persone che abbiano il diritto di prendere conoscenza di tali documenti. I documenti delicati sono iscritti nel registro o divulgati solo con il consenso dell'originatore.

Per facilitare l'accesso ai documenti, ciascuna Istituzione rende accessibile un registro di documenti, il quale è disponibile in forma elettronica.

[49] Per "documenti delicati" si intendono quei documenti provenienti dalle istituzioni o dalle agenzie da loro istituite, da Stati membri, paesi terzi o organismi internazionali, classificati come MOLTO SEGRETI/TOP SECRET, SEGRETI o RISERVATI.

7.VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

7.1 Cenni generali

La valutazione di impatto sulla protezione dei dati (DPIA, nell'acronimo inglese, *Data Protection Impact Assessment*) è stata introdotta dall'art. 35 Regolamento (UE) 2016/679[50] e consiste in una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali.

La valutazione è uno strumento molto importante in termini di *accountability*, in quanto aiuta il titolare in primis a rispettare le prescrizioni del Regolamento e in secondo luogo a dimostrare l'adozione di misure idonee a garantirne il rispetto; pertanto la DPIA è senza dubbio una procedura che permette di realizzare e dimostrare la conformità con le norme[51].

Nonostante il Regolamento, come abbiamo già avuto occasione di constatare con riferimento ad altri argomenti, non fornisca una definizione specifica di DPIA, tuttavia ne individua il contenuto minimo (art. 35 paragrafo 7). La DPIA, pertanto, deve riportare:

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[52];

---

[50] Anche l'art. 27 della Direttiva (UE) 2016/680, con riferimento alla protezione delle persone fisiche con riguardo al trattamento di dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, ha introdotto l'obbligo di effettuare una simile valutazione con riguardo a un trattamento «che può presentare un rischio elevato per i diritti e le libertà delle persone fisiche».

[51] Il valore e il ruolo della DPIA sono chiariti nel Considerando 84 dove si legge: «Per potenziare il rispetto del presente regolamento qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio. L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento. Laddove la valutazione d'impatto sulla protezione dei dati indichi che i trattamenti presentano un rischio elevato che il titolare del trattamento non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, prima del trattamento si dovrebbe consultare l'autorità di controllo.»

[52] Quando il Regolamento si riferisce a "diritti e libertà" degli interessati, il riferimento deve essere primariamente inteso come relativo al diritto alla privacy, ma può anche riguardare anche altri diritti fondamentali quali la libertà di espressione e di pensiero, la libertà di movimento, il divieto di discriminazioni, il diritto alla libertà di coscienza e di religione.

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 Regolamento, tenuto conto dei diritti degli interessi legittimi degli interessati e delle altre persone in questione.

Oltre al contenuto minimo, il Regolamento prevede anche una serie di sanzioni per l'inosservanza degli obblighi concernenti la DPIA; contravvenire al Regolamento, infatti, può comportare l'imposizione di sanzioni pecuniarie da parte della competente autorità di controllo. Le infrazioni possono consistere nel mancato svolgimento della DPIA quando il trattamento è soggetto a tale valutazione, nello svolgimento non corretto di una DPIA o nella mancata consultazione dell'autorità di controllo competente ove ciò sia necessario. La loro commissione può comportare l'irrogazione di una sanzione amministrativa pecuniaria fino a un massimo di €. 10 milioni ovvero – qualora si tratti di un'impresa – fino al 2% del fatturato mondiale annuo dell'esercizio finanziario precedente, se superiore a €. 10 milioni.

Lo svolgimento di una DPIA non è obbligatorio per ogni singolo trattamento. La valutazione è infatti necessaria solo se il trattamento «può comportare un rischio elevato[53] per i diritti e le libertà delle persone fisiche». Il fatto però di non essere obbligati a procedere a una DPIA, per mancanza delle condizioni necessarie[54], non solleva i titolari dal mettere in atto misure finalizzate a gestire in modo idoneo i rischi per i diritti e le libertà degli interessati – obbligo generale cui essi soggiacciono – attraverso la valutazione continua dei rischi creati dai propri trattamenti così da individuare quelle situazioni in cui una determinata tipologia di trattamenti «può presentare un rischio elevato per i diritti e le libertà delle persone fisiche».

Una DPIA può certamente riguardare un singolo trattamento, ma anche più trattamenti che presentano analogie tra loro in termini di natura, ambito contesto finalità e rischi. L'art. 35 paragrafo 1, infatti, è molto chiaro sul punto: «una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi». Anche il Considerando 92 affronta il tema della pluralità di trattamenti analoghi e rileva la possibilità che vi siano «circostanze in cui può essere ragionevole ed economico effettuare una valutazione d'impatto sulla protezione dei dati che verta su un oggetto più ampio di un unico progetto, per esempio quando autorità pubbliche o enti pubblici intendono istituire un'applicazione o una piattaforma di trattamento comuni o quando diversi titolari del trattamento progettano di introdurre un'applicazione o un ambiente di trattamento comuni in un settore o segmento industriale o per una attività trasversale ampiamente utilizzata.

Le valutazioni di impatto sulla protezione dei dati mirano a svolgere un'analisi sistematica di situazioni nuove che potrebbero comportare rischi elevati per i diritti e le libertà delle persone fisiche; pertanto non occorre condurre una DPIA per quei trattamenti – svolti in un contesto specifico e per una specifica finalità – che siano già stati oggetto di analisi. Si pensi ad esempio all'utilizzo di tecnologie simili per raccogliere le stesse tipologie di dati per identiche finalità.

---

[53] Per "rischio" si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità. Infatti la "gestione del rischio" è definibile come l'insieme coordinato delle attività finalizzate a guidare e monitorare un ente o organismo nei riguardi di tale rischio.

[54] Qualora non emerga con chiarezza la necessità di una DPIA, il WP29 nelle Linee guida elaborate sul punto raccomanda comunque di farvi ricorso, in quanto la DPIA contribuisce all'osservanza delle norme in materia di protezione dati da parte dei titolari di trattamento.

Quando un trattamento è svolto in contitolarità (art. 26 Regolamento) è necessario che ciascun titolare definisca con precisione gli obblighi rispettivamente incombenti. La DPIA dovrebbe stabilire chi ha la responsabilità delle singole misure finalizzate alla gestione dei rischi e alla tutela dei diritti e delle libertà degli interessati. Ciascun titolare dovrebbe indicare con chiarezza le rispettive esigenze e condividere tutte le informazioni utili senza pregiudicare quanto coperto da segreto né rivelare eventuali vulnerabilità. L'art. 26 evidenzia il concetto che il trasparente accordo interno fra i contitolari del trattamento è prevalentemente volto a garantire all'interessato di poter esercitare i propri diritti e definire chi dei contitolari dovrà provvedere a fornire, al momento della raccolta, le informazioni previste per l'ottenimento dei dati personali, indipendentemente dal contenuto dell'accordo interno; nonostante ciò, l'interessato può esercitare i propri diritti nei confronti e contro ciascun titolare del trattamento (art. 26 parag. 3). Il contenuto essenziale dell'accordo interno tra i titolari di uno stesso trattamento deve essere messo a disposizione dell'interessato, così come disposto dal paragrafo 2 dell'art. 26, ma non è richiesto che l'accordo stesso sia fornito o reso accessibile agli interessati. In ogni caso queste informazioni dovranno comunque essere fornite con le informazioni previste dagli artt. 13 e 14.

Sotto il profilo pratico dell'individuazione del contitolare, non ci sono differenze rispetto alle modalità con le quali si identifica il titolare del trattamento. In caso di controversie sull'identificazione di titolare e contitolare – o meglio sulla differenziazione delle figure – è necessario applicare il criterio di disambiguazione enunciato dal Garante privacy nella sua prescrizione del 29 Aprile 2009[55]. Tale principio afferma che è titolare del trattamento chi effettua scelte e prende decisioni inerenti le finalità dei trattamenti, impartisce decisioni o direttive vincolanti ed esercita funzioni di controllo. Pertanto, è da considerare "titolare del trattamento" chi esercita l'effettivo potere decisorio.

Come già detto la DPIA si rende necessaria ogniqualvolta un trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone e l'art. 35 parag. 3 esemplifica – senza pretese di esaustività – alcuni casi in cui questo può verificarsi[56]:

a) Qualora debba essere effettuata 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) Nel caso di trattamento, su larga scala, di categorie particolari di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o di dati relativi a condanne penali e a reati di cui all'articolo 10; ovvero

c) Qualora si voglia effettuare la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

[55] Si tratta del [doc. web n. 1617709] Servizi postali: Poste Italiane resta titolare del trattamento anche in caso di appalto – 29 aprile 2009, rinvenibile all'indirizzo http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1617709

[56] Si vedano anche i Considerando n. 75, 76, 92 e 116 per altri esempi relativi a trattamenti che possono presentare un rischio elevato.

L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68[57].

Oltre ai tre esempi forniti dal legislatore europeo, il Gruppo di lavoro sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali (WP29) ha stilato una lista di nove criteri – mettendo in sistema quando disposto dall'art. 35 e quanto rilevato nei Considerando 71, 75 e 76 – sulla base dei quali è possibile identificare altri casi di trattamenti che possono presentare un rischio elevato:

1. Trattamenti valutativi o di *scoring*, compresa la profilazione e le attività predittive, in particolare a partire da «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». Ad esempio è il caso di una società che crei profili comportamentali o di marketing a partire dalle operazioni o dalla navigazione compiute sul proprio sito web.
2. Decisioni automatizzate che producono significativi effetti giuridici o di analoga natura: il riferimento è a trattamenti finalizzati ad assumere decisioni in grado di produrre «effetti giuridici sulla persona fisica» ovvero che «incidono in modo analogo significativamente su dette persone fisiche» (art. 35 parag. 3 lett. a)). Per esempio il trattamento può comportare l'esclusione di una persona fisica a determinati benefici ovvero la sua discriminazione; il trattamento che produce effetti minimi o nulli su un interessato non soddisfa questo specifico criterio.
3. Monitoraggio sistematico: è il caso di trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o «la sorveglianza sistematica[58] di un'area accessibile al pubblico» (art. 35 parag. 3 lett. c)). Una simile raccolta può comportare un rischio elevato in quanto può avvenire in circostanze tali da non consentire agli interessati di comprendere chi vi stia procedendo e per quali finalità; inoltre è quasi sempre impossibile, per gli interessati, sottrarsi a questa tipologia di trattamenti in aree pubbliche o, comunque, pubblicamente accessibili[59].
4. Dati sensibili o dati di natura estremamente personale che sono elencati negli artt. 9 e 10 del Regolamento[60]. Al di là dell'elencazione del Regolamento, vi sono alcune categorie di dati che possono aumentare gli eventuali rischi per i diritti e le libertà delle persone fisiche. Si tratta di dati personali considerati sensibili – nell'accezione comune del termine – perché connessi alla vita familiare o privata[61] ovvero in quanto incidono sull'esercizio di un diritto fondamentale[62] ovvero, da ultimo, in quanto una

[57] Si veda *supra* cap. 6.7.
[58] Per "sistematico" si deve intendere qualcosa che avviene per sistema; predeterminato, organizzato o metodico; che ha luogo nell'ambito di un progetto complessivo di raccolta di dati; svolta nell'ambito di una strategia.
[59] Per "area pubblicamente accessibile" si intende un luogo aperto alla generalità delle persone, per esempio una piazza, un centro commerciale, una strada, una biblioteca.
[60] Si tratta di dati personali in grado di rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona., o di dati relativi a condanne penali e a reati o a connesse misure di sicurezza.
[61] Come ad esempio i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza.
[62] Come i dati relativi al tracciamento della propria posizione, la cui raccolta incide sulla libertà di circolazione.

loro violazione possa comportare un grave impatto sulla vita quotidiana dell'interessato[63]. A tale proposito può essere necessario indagare se tali dati siano già stati resi pubblici dall'interessato o da terzi perché, in tal caso, la pubblicità può essere un elemento da esaminare nel valutare l'aspettativa di un utilizzo ulteriore di tale dato per determinati scopi. Un tale criterio, specifica il WP29, può riferirsi anche a dati quali documenti personali, e-mail, agende (cartacee ed elettroniche) e informazioni molto personali contenute in applicazioni che consentono di tenere traccia del proprio stile di vita.

5. Trattamenti di dati su larga scala: come in altri casi, anche con riferimento al concetto di "larga scala" il regolamento non ci offre una definizione[64], ma ancora una volta è il WP29 a fornire alcuni fattori da considerare per stabilire se un trattamento sia svolto su larga scala. A tal fine vanno considerati: il numero di soggetti interessati dal trattamento – in termini numerici o di percentuale rispetto alla popolazione di riferimento –; il volume dei dati e/o l'ambito delle diverse tipologie di dati oggetto di trattamento; la durata o la persistenza dell'attività di trattamento; infine, l'ambito geografico dell'attività di trattamento;

6. Combinazione o raffronto di insiemi di dati, per esempio derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato[65].

7. Dati relativi a interessati vulnerabili[66]: il trattamento di questa tipologia di informazioni rappresenta un criterio ai fini della DPIA in quanto è più accentuato lo squilibrio di poteri fra interessato e titolare del trattamento, nel senso che il singolo può non disporre del potere di acconsentire (o di opporsi) con facilità al trattamento dei propri dati né può talora con facilità esercitare i propri diritti. La categoria

---

[63] Come ad esempio i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti.

[64] Alcune indicazioni in merito sono contenute nel Considerando 91 intendendo per tali quelli «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».

[65] A tal proposito le Linee guida del WP29 sul principio di limitazione della finalità (13/EN WP 2003, p. 24) ci consentono di svolgere alcune riflessioni. Il problema che si pone in merito alla compatibilità delle finalità è dato dal modo in cui una persona ragionevole, nella situazione della persona interessata, si aspetta vengano utilizzati i suoi dati in base al contesto della raccolta. Viene quindi alla luce un aspetto importante, vale a dire la natura della relazione tra controllore e interessato. Affinché una tale relazione sia "buona" sarebbe necessario procedere non solo a una revisione di tutte le dichiarazioni legali già fatte, ma anche esaminare che sarebbe prassi consuetudinaria e generalmente prevista tanto in quel determinato contesto quanto in quel determinato rapporto (commerciale o altro).
In generale, è possibile trarre dalle Linee guida, il rigore nella valutazione della compatibilità delle finalità dei trattamenti deve essere inversamente proporzionale al grado di libertà di scelta dell'interessato, alla specificità dei termini del consenso e/o alla discutibilità dell'ulteriore uso dei dati. In altre parole, tanto meno l'interessato è stato libero di scegliere, i termini non sono specifici e/o sia discutibile l'ulteriore utilizzo, tanto più dovrà essere rigorosa la valutazione.

[66] Si riporta integralmente il Considerando 75 il quale, in tema di vulnerabilità degli interessi, procede a un'elencazione delle situazione dalle quali possono derivare rischi per i diritti e le libertà delle persone fisiche.
«I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione 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, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

degli interessati vulnerabili comprende anche i minori, che si può ritenere non siano in grado di opporsi o acconsentire, in modo consapevole e ragionato, al trattamento dei propri dati personali, i dipendenti, quei segmenti di popolazione particolarmente vulnerabile e meritevole di specifica tutela (soggetti con patologie psichiatriche, richiedenti asilo, anziani, pazienti) e ogni interessato per il quale si possa identificare una situazione di disequilibrio nel rapporto con il rispettivo titolare del trattamento.

8. Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative, come l'associazione fra tecniche dattiloscopiche e riconoscimento del volto per migliorare il controllo degli accessi fisici, e così via. Il Regolamento chiarisce (art. 35 paragrafo 1 e Considerando 89 e 91) che l'utilizzo di una nuova tecnologia , definito «in conformità con il grado di conoscenze tecnologiche raggiunto», può comportare l'obbligo di condurre una DPIA, in quanto il ricorso a una nuova tecnologia può generare forme innovative di raccolta e utilizzo dei dati cui può associarsi un rischio elevato per i diritti e le libertà delle persone. Nei fatti, le conseguenze sul piano individuale e sociale del ricorso a una nuova tecnologia sono talora ignote. La DPIA aiuterà il titolare a comprendere e gestire tali rischi. Per esempio, lacune applicazioni legate all'I*nternet Of Things* potrebbero avere impatti significativi sulla vita privata e le abitudini delle persone e, quindi, necessitano di una DPIA.

9. Tutti quei trattamenti che, di per sé, «impediscono [agli interessati] di esercitare un diritto o di avvalersi di un servizio o di un contratto» (art. 22 e Considerando 91). Ciò comprende i trattamenti finalizzati a consentire, modificare o negare l'accesso degli interessati a un servizio o la stipulazione di un contratto.

   Si pensi, a titolo di esempio, allo screening dei clienti di una banca attraverso i dati registrati in una centrale rischi al fine di stabilire se ammetterli o meno a un finanziamento.

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 WP29 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. Tuttavia, in alcuni casi un titolare può ritenere che un trattamento che soddisfa solo uno dei criteri di cui sopra necessiti di una DPIA.

È anche possibile che, nonostante il trattamento soddisfi uno o più dei criteri sopra enunciati, a giudizio del titolare non presenti un rischio elevato e quindi non necessiti di una DPIA. In questo caso, lo stesso titolare dovrà motivare e documentare la scelta della mancata conduzione della DPIA, allegando o annotando l'opinione della protezione dei dati. Una tale facoltà gli è conferita in forza del principio di responsabilizzazione il quale prevede, inoltre, che ciascun titolare tenga un registro delle attività di trattamento svolte sotto la propria responsabilità, comprendente:

- √ Le finalità del trattamento;
- √ Una descrizione delle categorie di dati e i destinatari dei dati stessi;
- √ Una descrizione generale, ove possibile, delle misure di sicurezza tecniche e organizzative di cui all'art. 32 parag. 1;

Le autorità di controllo sono tenute a redigere, pubblicare e comunicare al Comitato europeo per la protezione dei dati un elenco dei trattamenti che necessitano di una DPIA, così come disposto dall'art. 35 parag. 4. Al riguardo, il successivo parag. 6, prevede che l'autorità di controllo competente applichi «il meccanismo di coerenza di cui all'art. 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri o, ancora, attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.».

Così come è possibile stabilire quando una DPIA sia necessaria, lo è anche definire i casi – oltre al giudizio del titolare – in cui non lo sia:

- √ Se il trattamento non «può comportare un rischio elevato per i diritti e le libertà di persone fisiche» (art. 35 parag. 1);
- √ Se la natura, l'ambito, il contesto e le finalità del trattamento sono molto simili a quelli del trattamento per cui è già stata condotta una DPIA. In casi del genere si possono utilizzare i risultati della DPIA per trattamenti analoghi;
- √ Se il trattamento è stato sottoposto a verifica da parte di un'autorità di controllo prima del 25 Maggio 2018 in condizioni specifiche che non hanno subito modifiche[67];
- √ Se un trattamento, conformemente con la lettera c) o e) dell'art. 6 parag. 1, trova la propria base nel diritto dell'Unione europea o di uno Stato membro, la base legale in questione disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta (art. 35 parag. 10)[68], tranne ove uno Stato membro abbia previsto la necessità di condurre una DPIA per i trattamenti pregressi;
- √ Se il trattamento è compreso nell'elenco facoltativo (redatto dall'autorità di controllo ai sensi dell'art. 35 parag. 5) dei trattamenti per i quali non è necessario procedere alla DPIA. Tale elenco può riguardare trattamenti conformi alle condizioni specificate dalla singola autorità, in particolare attraverso linee guida, decisioni o autorizzazioni specifiche, norme di conformità e via discorrendo. In casi del genere, salvo riesame da parte della competente autorità di controllo, la DPIA non è necessaria; ciò alla sola condizione, però, che il trattamento ricada nello specifico ambito della procedura menzionata nell'elenco e continui a risultare pienamente conforme ai relativi requisiti stabiliti dal Regolamento.

[67] Nel Considerando 171, a riguardo, si legge che: «Le decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla Direttiva 95/46/CE restano in vigore fino a quando non vengono modificate, sostituite o abrogate».

[68] Si osservi che, qualora sia stata condotta una DPIA nella fase di elaborazione dello strumento che offre la base legale per il trattamento, è probabile che sia necessario un riesame prima dell'entrata in vigore poiché lo strumento giuridico adottato può differire da quello proposto in misura tale da incidere sull'impatto in termini di privacy e protezione dei dati. Inoltre, può darsi che non siano disponibili sufficienti informazioni di ordine tecnico rispetto al trattamento in quanto tale al momento dell'adozione dello strumento normativo suddetto, anche se accompagnato da una DPIA; in casi del genere, può risultare comunque necessario condurre una DPIA specifica prima di procedere al trattamento vero e proprio.

Nel caso di trattamenti già in corso, l'obbligo di condurre una DPIA vige solo per quelli che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche e per i quali siano intervenute variazioni dei rischi tenuto conto della natura, dell'ambito, del contesto e delle finalità dei trattamenti stessi. Non è necessario condurre una DPIA per quei trattamenti che siano stati oggetto di verifica preliminare da parte del Garante per la protezione dei dati personali e che proseguano con le stesse modalità oggetto di tale verifica. Come indicato nel considerando 171, «le decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla Direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate.».

I trattamenti tendono a evolvere rapidamente e possono facilmente presentarsi nuove vulnerabilità; pertanto potrebbe rivelarsi utile la revisione di una DPIA in primis in funzione di un miglioramento continuo e, in secondo luogo, per mantenere inalterato il livello di protezione dei dati al mutare delle condizioni nel tempo.

7.2 Come si effettua una DPIA

In primo luogo bisogna fare attenzione alla scelta dei tempi: normalmente la DPIA viene condotta «prima di procedere al trattamento», così come disposto dall'art. 35 parag. 1 e 10 e suggerito nei Considerando 80 e 93, tranne quando si è in presenza di un trattamento già in corso sottoposto a verifica preliminare dell'autorità di controllo; in quest'ultimo caso la DPIA dovrebbe essere condotta prima di apportare modifiche significative al trattamento stesso. Lo svolgimento della DPIA è un processo continuativo e non un'attività *una tantum*, pertanto non è ragionevole differire – o addirittura evitare di condurre – una DPIA per il solo fatto che potrebbe rendersi necessario un suo aggiornamento dopo l'inizio effettivo del trattamento. L'aggiornamento continuo della DPIA, infatti, non può che garantire la dovuta considerazione delle tematiche legate alla privacy e alla protezione dei dati, favorendo l'individuazione di soluzioni dirette a promuovere l'osservanza delle norme contenute nel nuovo Regolamento.

Per quanto riguarda la conduzione della DPIA, il titolare del trattamento è tenuto a garantirne l'effettuazione (art. 35 parag. 2) mentre la conduzione materiale vera e propria potrà anche essere affidata a un altro soggetto, interno o esterno all'organismo. Va da sé che la responsabilità ultima dell'adempimento rimane in carico al titolare del trattamento. Se è stato designato un RPD, questi dovrà essere consultato dal titolare; di tale consultazione – e delle conseguenti decisioni – deve esserne data informazione nell'ambito della DPIA. Il RPD deve altresì monitorare lo svolgimento della DPIA[69]. Qualora il trattamento sia svolto, in tutto o in parte, da un responsabile questi dovrà assistere il titolare nella conduzione della DPIA, fornendo ogni informazione necessaria per garantire il rispetto degli obblighi di cui agli artt. 32-36 e tenendo conto della natura del trattamento e delle informazioni a sua disposizione (art. 28 parag. 3 lett. f)).

Secondo quanto disposto dall'art. 35 parag. 9, il titolare del trattamento «se del caso, raccoglie le opinioni degli interessati e dei loro rappresentati sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti». A tal proposito il WP 29 fa alcune precisazioni:

[69] Sull'argomento sono rinvenibili ulteriori informazioni nella parte sul Responsabile per la Protezione dei dati (cap. 6.4).

Per la raccolta delle opinioni si possono individuare molteplici modalità, in rapporto al contesto: per esempio, uno studio generico relativo a finalità e mezzi del trattamento; un quesito rivolto ai rappresentanti del personale; un questionario inviato ai futuri clienti del titolare. Il titolare dovrà accertarsi dell'esistenza di una base legale per il trattamento di dati personali eventualmente connesso alla raccolta di tali opinioni, quando il consenso al trattamento in questione non può rappresentare una modalità idonea per raccogliere le opinioni degli interessati.

Qualora la decisione assunta in ultima analisi dal titolare si discosti dall'opinione degli interessati, è bene che il titolare documenti le motivazioni che hanno condotto alla prosecuzione o meno del progetto;

Il titolare dovrebbe inoltre documentare le motivazioni della mancata consultazione degli interessati, qualora decida che quest'ultima non sia opportuna, ad esempio perché potrebbe pregiudicare la riservatezza dei piani aziendali oppure perché sarebbe sproporzionata o impraticabile.

Per quanto riguarda invece la metodologia che deve essere applicata per condurre una DPIA – la metodologia può non essere unica, ma i criteri dovranno essere gli stessi – il Regolamento fissa le sue caratteristiche basilari nell'art. 35 parag. 7 e nei Considerando 84 e 90. Si legge infatti che la valutazione deve contenere almeno:

Una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento: si deve tenere conto della natura, dell'ambito, del contesto e delle finalità del trattamento. Dovranno essere indicati i dati personali oggetto del trattamento i destinatari e il periodo di conservazione previsto dei dati stessi. Inoltre, si dà una descrizione funzionale del trattamento, si specificano gli strumenti utilizzati (hardware, software, reti, persone, supporti o canali di trasmissione cartacei) e si terrà conto dell'osservanza di eventuali codici di condotta approvati.

Una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità. Dovranno pertanto essere definite le misure previste per rispettare il Regolamento tenendo conto delle misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di finalità specifiche, esplicite e legittime, della liceità del trattamento, dei dati adeguati, pertinenti e limitati a quanto necessario e al periodo limitato di conservazione. Si dovrà inoltre tenere conto delle misure che contribuiscono ai diritti degli interessati, come: le informazioni fornite agli interessati, il diritto di accesso e portabilità dei dati, il diritto di rettifica e cancellazione, quello di opposizione e limitazione del trattamento, i rapporti con i responsabili del trattamento, le garanzie per i trasferimenti internazionali di dati, la consultazione preventiva.

Una valutazione – e relativa gestione attraverso la previsione di misure idonee – dei rischi per i diritti e le libertà degli interessati persone fisiche. Si determinano l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio dal punto di vista degli interessati. Si dovrà pertanto tenere conto delle fonti di rischio, si dovranno identificare gli impatti potenziali sui diritti e le libertà degli interessati in caso, ad esempio, di accesso illegittimo, modifiche indesiderate e indisponibilità dei dati e, da ultimo, si procederà a una stima di probabilità e gravità.

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 Regolamento, tenuto conto dei diritti e

degli interessi legittimi degli interessati e delle altre persone in questione, i quali potranno essere sentiti, anche per tramite di loro rappresentanti.

Per concludere, in tema di pubblicità della DPIA si rileva come la sua pubblicazione non costituisca un obbligo formale ai sensi del Regolamento ma sia rimessa più semplicemente alla discrezionalità del titolare del trattamento. Sarebbe però opportuno, secondo il WP29, che i titolari rendessero pubbliche una sintesi o almeno le conclusioni della DPIA[70]: in tal modo promuoverebbero la fiducia nelle loro attività di trattamento, dando prova di un approccio responsabile e trasparente.

[70] Non è necessaria la pubblicazione integrale della DPIA, specialmente qualora essa contenga informazioni dettagliate rispetto ai rischi di sicurezza che investono il titolare ovvero nel caso in cui possa rivelare segreti commerciali o informazioni di rilevanza commerciale. In questi casi può essere sufficiente una sintesi delle principali risultanze del processo di valutazione di impatto o anche una semplice dichiarazione relativa all'effettuazione di una DPIA.

8.OBBLIGHI DEL TITOLARE

8.1 Registri delle attività di trattamento

L'art. 30 prevede che le imprese o organizzazioni con più di 250 dipendenti tengano un registro nel quale devono essere annotate determinate informazioni. Sotto tale limite numerico, pertanto, non sussiste l'obbligo, salvo che il trattamento effettuato possa presentare un rischio per i diritti e le libertà dell'interessato ovvero non sia occasionale o includa il trattamento di categorie particolari dati come quelli sensibili o giudiziari.

Secondo quanto disposto dall'art. 30 ogni titolare del trattamento e l'eventuale rappresentante (ove presente), si diceva, tengono un registro delle attività di trattamento svolte sotto la propria responsabilità contente le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e di ogni contitolare del trattamento, del rappresentante del titolare del trattamento e dell'eventuale responsabile della protezione dei dati;

b) Le finalità del trattamento;

c) Una descrizione delle categorie di interessati e delle categorie di dati personali;

d) Le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi;

e) Ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale e, per i trasferimenti di cui all'art. 49 co. 2, la documentazione della 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.

Non solo il titolare, ma anche ogni responsabile del trattamento (e il suo eventuale rappresentante) tengono un registro di tutte le categorie di attività di trattamento dei dati personali svolte per conto di un titolare del trattamento, contenente:

a) Nome e dati di contatto del responsabile o dei responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentate del titolare del trattamento o del responsabile del trattamento e dell'eventuale 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 all'art. 49 co 2, la documentazione delle garanzie adeguate;

d) Ove possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative.

Su richiesta, il titolare del trattamento o il responsabile del trattamento e l'eventuale rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

8.2 Sicurezza del trattamento

Per mantenere la sicurezza e prevenire trattamenti che possono violare il Regolamento, il titolare del trattamento e il responsabile dovrebbero valutare i rischi inerenti al trattamento e attuare misure per limitarli, come ad esempio la cifratura. Tali misure, continua il legislatore nel Considerando 83 e conferma nell'art. 32 parag. 1, dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello Stato dell'arte e dei costi di attuazione rispetto ai rischi che rappresentano i trattamenti oltre che della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche. Per questi motivi, come si diceva all'inizio, il titolare e il responsabile mettono in atto misure concrete che comprendono, tra le altre:

√ La pseudonimizzazione e la cifratura dei dati personali;

√ La capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

√ La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

√ Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare il livello di sicurezza perpetrato con queste misure, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. È possibile fornire, sempre al fine di valutare l'efficacia delle misure adottate, la prova dell'adesione a un codice di condotta – approvato ai sensi dell'art. 40 – o a un meccanismo di certificazione approvato.

8.3 *Data Breach* e comunicazione all'interessato

In caso di violazione dei dati personali o *Data Breach*[71], dispone l'art. 33, il titolare del trattamento **notifica la violazione all'autorità di controllo** competente 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, deve essere corredata dei motivi del ritardo.

La notifica dovrà essere in grado almeno di:

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.

Qualora non dovesse essere possibile fornire nell'immediatezza le informazioni appena elencate, queste potranno essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Il successivo art. 34, invece, prevede un'altra importante incombenza collegata alla notifica all'autorità di controllo, vale a dire la **comunicazione di una violazione dei dati personali all'interessato**. Quando infatti 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. Tale comunicazione dovrà descrivere con un linguaggio semplice e chiaro la natura della violazione e contenere le informazioni e le misure sopra elencate ai punti b), c) e d).

La comunicazione però non è richiesta, specifica il legislatore nel paragrafo 3, qualora sia soddisfatta una delle seguenti condizioni:

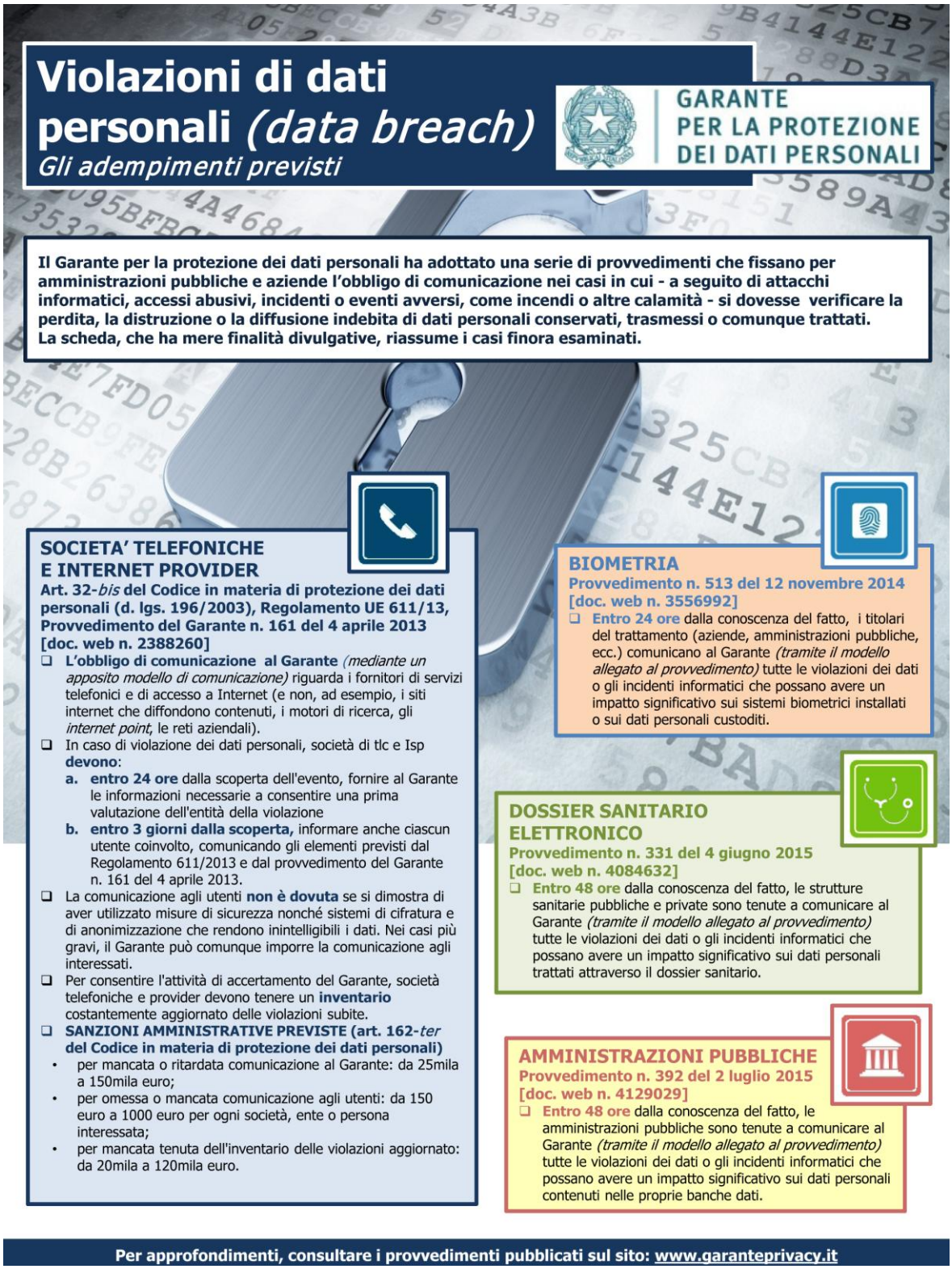
1) Il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

[71] Con il termine *Data Breach* si intende un incidente di sicurezza in cui i dati personali vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato. Solitamente la violazione si realizza con una divulgazione dei dati riservati o confidenziali all'interno di un ambiente privo di misure di sicurezze, come ad esempio sul web, in maniera involontaria o volontaria. Tale divulgazione può avvenire in seguito a: perdita accidentale del supporto sul quale sono conservati i dati (penna usb o hd esterno), furto, infedeltà aziendale, accesso abusivo ai sistemi informatici.

2) Il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

3) Detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Da ultimo si rileva come il Garante per la protezione dei dati personali abbia adottato negli ultimi anni una serie di provvedimenti che introducono in determinati settori l'obbligo di comunicare eventuali violazioni di dati personali all'Autorità stessa e, in alcuni casi, anche ai soggetti interessati. Il mancato o ritardato adempimento della comunicazione espone, superfluo a dirsi, alla possibilità di sanzioni amministrative.



8.4 Certificazione

Al fine di migliorare la trasparenza e il rispetto del regolamento, si legge nel Considerando 100 e nell'art. 42, viene incoraggiata l'istituzione di meccanismi di certificazione, di sigilli e di marchi di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi. La certificazione – volontaria e accessibile tramite una procedura trasparente – è rilasciata da appositi organismi di certificazione (art. 43) o dall'autorità di controllo competente in base ai criteri approvati da questa o dal comitato.

La certificazione è rilasciata al titolare o al responsabile del trattamento per un periodo massimo di tre anni e può essere rinnovata alle stesse condizioni purché continuino a essere soddisfatti i requisiti pertinenti. Al pari, la certificazione può non essere rilasciata ovvero può essere revocata qualora non siano o non siano più soddisfatti i requisiti per la certificazione.

Il comitato raccoglie in un registro tutti i meccanismi di certificazione e i sigilli e i marchi di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato.

8.5 Sanzioni

Il Gruppo di lavoro WP29, costituito dai Garanti della protezione dei dati personali degli Stati membri, ha stilato il 03.10.2017 delle Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del Regolamento (UE) n. 2016/679[72]. Nonostante il documento sia dichiaratamente indirizzato all'autorità di controllo competente per coadiuvarla – una volta accertata la violazione – nella individuazione della (o delle) misure correttive più appropriate per affrontare tale violazione, può essere utile analizzarne il contenuto per comprendere quali siano gli strumenti a disposizione dell'Autorità e i passaggi logici che questa compie nell'affrontare le diverse violazioni al Regolamento.

Le autorità di controllo, nel ricorrere ai poteri che l'art. 58, parag. 2, lett. da b) a j) attribuisce loro per far fronte a un'inadempienza da parte di un titolare del trattamento, devono osservare i seguenti principi:

1. **La violazione del regolamento dovrebbe comportare l'imposizione di "sanzioni equivalenti"**. Sul punto i Considerando 10 e11 evidenziano come, «al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, il livello di protezione dovrebbe essere equivalente in tutti gli Stati membri»; per garantire un livello equivalente di protezione in tutta l'Unione – prosegue il Considerando 11 – occorrono «poteri equivalenti per controllare e assicurare il rispetto delle norme di protezione dei dati personali e sanzioni equivalenti per le violazioni negli Stati membri». Non solo, sanzioni equivalenti in tutti gli Stati membri

[72] Il documento, tradotto in italiano, è reperibile al seguente indirizzo http://194.242.234.211/documents/10160/0/WP+253++Linee+guida+sanzioni+amministrative+pecuniarie+Reg+UE+2016+679

e una cooperazione efficace tra le autorità di controllo dei diversi stati membri sono considerate un modo per «prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno».

2. Come tutte le misure correttive scelte dalle autorità di controllo, le sanzioni amministrative pecuniarie dovrebbero essere "effettive, proporzionate e dissuasive". Il principio è esplicitato nell'art. 83 parag. 1. Al fine di irrogare sanzioni che siano tali l'autorità di controllo – qualora i destinatari delle sanzioni siano imprese – deve rifarsi alla definizione della nozione di impresa fornita dalla Corte di giustizia dell'Unione europea ai fini dell'applicazione degli artt. 101-102 TFUE[73] secondo cui il concetto di impresa va inteso come un'unità economica che può essere composta dall'impresa madre e da tutte le filiali coinvolte. Quindi, conformemente al diritto e alla giurisprudenza dell'UE, un'impresa deve essere intesa quale unità economica che intraprende attività economiche e/o commerciali, a prescindere dalla persona giuridica implicata[74].

3. L'autorità di controllo competente effettuerà una valutazione "in ogni singolo caso".

4. Un approccio armonizzato alle sanzioni amministrative pecuniarie in materia di protezione dei dati richiede la partecipazione attiva delle autorità di controllo e lo scambio di informazioni tra le stesse. Le autorità di controllo collaborano tra loro e, ove necessario, con la Commissione europea tramite il meccanismo di cooperazione, come stabilito nel Regolamento, al fine di sostenere scambi formali e informali di informazioni, ad esempio attraverso seminari periodici. Tale cooperazione, prosegue il WP29 nelle Linee guida, si concentrerà sulla loro esperienza e pratica nell'applicazione dei poteri sanzionatori al fine di raggiungere una maggiore coerenza.

L'art. 83 parag. 2 elenca una serie di elementi che devono essere tenuti in considerazione dalle autorità di controllo, tanto nell'irrogazione della sanzione amministrativa quanto nella determinazione del relativo importo. Quello che ha voluto fare il gruppo di Garanti europei è stato fornire orientamenti alle autorità di controllo su come interpretazione le singole circostanze del caso alla luce di tali elementi.

a) **Natura, gravità e durata della violazione**. Il regolamento non fissa un importo specifico per violazione specifiche, ma solo un massimale. Da ciò si può desumere la gravità relativamente minore delle violazioni di cui all'art. 83 parag. 4 rispetto a quelle del parag. 5. A proposito il WP29 fa notare come, in determinate circostanze, le violazioni del regolamento che per natura dovrebbero rientrare nella categoria «fino a 10 000 000 EUR o [...] fino al 2 % del fatturato mondiale totale annuo» conformemente all'articolo 83, paragrafo 4, potrebbero essere classificate in una categoria superiore (20 milioni di EUR). È il caso, ad esempio, di una violazione che sia stata precedentemente oggetto di un

[73] I due articoli in questione disciplinano le regole di concorrenza applicabili alle imprese.
[74] A titolo esemplificativo si citano due sentenze della Corte di Giustizia. Nella causa Höfner e Elsner (punto 21, ECLI:EU:C:1991:161) la Corte dispone che «la nozione di impresa abbraccia qualsiasi entità che esercita un'attività economica, a prescindere dallo status giuridico di detta entità e dalle sue modalità di finanziamento». Nella causa Confederación Española de Empresarios de Estaciones de Servicio, (punto 40, ECLI:EU:C:2006:784), invece, la Corte ritiene che un'impresa debba essere «intesa nel senso che essa si riferisce ad un'unità economica, anche qualora, sotto il profilo giuridico, questa unità economica sia costituita da più persone, fisiche o giuridiche».

ordine – ex art. 58 parag. 2 – dell'autorità di controllo che il titolare o il responsabile del trattamento non ha rispettato (art. 83, parag. 6)[75].

b) **Carattere doloso o colposo della violazione**. In generale, il "dolo" comprende sia la consapevolezza che l'intenzionalità in relazione alle caratteristiche di un reato, mentre per "colposo" si intende che non vi era l'intenzione di causa la violazione nonostante il titolare e/o il responsabile del trattamento abbiano violato l'obbligo di diligenza previsto per legge. È generalmente riconosciuto che le violazioni dolose, dalle quali emerge la non curanza delle disposizioni di legge, siano più gravi di quelle colpose e pertanto possano verosimilmente giustificare l'applicazione di una sanzione amministrativa pecuniaria. Tra le circostanze indicanti il carattere doloso di una violazione figura il trattamento illecito autorizzato esplicitamente dall'alta dirigenza del titolare del trattamento oppure effettuato nonostante i pareri del responsabile della protezione dei dati o ignorando le politiche esistenti, ad esempio ottenendo e trattando dati relativi ai dipendenti di un concorrente con l'intento di screditare tale concorrente sul mercato. Altri esempi forniti dal WP29 sono la modifica di dati personali per dare un'impressione positiva (e fuorviante) circa il conseguimento degli obiettivi[76] oppure lo scambio di dati personali con finalità di marketing, ossia vendita di dati come "approvati" senza verificare oppure ignorando il parere degli interessati circa le modalità di utilizzo dei propri dati. Altre circostanze, quali la mancata lettura e il non rispetto delle politiche esistenti, errore umano, mancata verifica dei dati personali nelle informazioni pubblicate, incapacità di apportare aggiornamenti tecnici in maniera puntuale, mancata adozione delle politiche o, più semplicemente, la loro mancata applicazione possono essere sintomo di negligenza.

c) Le misure adottate dal titolare del trattamento o al responsabile del trattamento per attenuare il danno subito dagli interessati. I titolari del trattamento e i responsabili del trattamento hanno l'obbligo di attuare misure tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio, di condurre valutazioni di impatto sulla protezione dei dati e di mitigare i rischi arrecati ai diritti e alle libertà personali dal trattamento dei dati personali. Tuttavia, quando si verifica una violazione e l'interessato ne subisce i danni, la parte responsabile dovrebbe fare quanto in suo potere per ridurre le conseguenze della violazione per il o i soggetti coinvolti. Un tale comportamento verrò preso in considerazione dall'autorità di controllo nel momento della scelta delle misure correttive e nel calcolo della sanzione da imporre nel caso specifico.

d) Il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli artt. 25 e 32. Il nuovo regolamento ha introdotto un livello di responsabilità del responsabile del trattamento ben superiore a quello vigente durante l'operatività della Direttiva 95/46/CE. Il grado di responsabilità del titolare del trattamento o del responsabile, valutato sulla base dell'adozione di una misura correttiva appropriata, può dipendere dal fatto che il titolare abbia attuato misure tecniche che seguono i principi della protezione dei dati fin dalla progettazione o per impostazione predefinita oppure misure organizzative

[75] L'applicazione dell'art. 83, parag. 6, deve necessariamente tenere conto del diritto procedurale nazionale. Il diritto nazionale determina le modalità di emissione e di notifica di un ordine, il momento di entrata in vigore e l'eventuale periodo di tolleranza per conformarvisi. In particolare, occorre tenere conto dell'effetto di un appello sull'esecuzione di un ordine.
[76] Questo episodio è stato riscontrato nel contesto degli obiettivi relativi ai tempi di attesa ospedalieri.

che attuano i principi della protezione dei dati fin dalla progettazione e per impostazione predefinita a tutti i livelli dell'organizzazione oppure che il titolare o il responsabile abbiano messo in atto un livello di sicurezza adeguato o ancora, infine, che le prassi e/o le politiche pertinenti in materia di protezione dei dati siano conosciute e applicate al livello adeguato di gestione dell'organizzazione.

e) **Eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento**. Questo criterio è utile a valutare i precedenti di colui che commette la violazione. L'autorità di controllo dovrebbe considerare la possibilità che la valutazione possa avere una portata piuttosto vasta, dal momento che ogni violazione del regolamento potrebbe essere pertinente ai fini della valutazione potendo fornire indicazioni su un livello generale di conoscenza insufficiente o di indifferenza nei confronti delle norme sulla protezione dei dati.

f) Il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi. Il regolamento non indica con precisione come tenere conto degli sforzi dei titolari del trattamento o dei responsabili nel rimediare a una violazione già accertata dall'autorità di controllo. Tuttavia, nello scegliere la misura correttiva proporzionata al singolo caso si dovrebbe tener conto anche dell'eventuale intervento con cui il titolare del trattamento abbia limitato o addirittura azzerato le ripercussioni negative sui diritti delle persone che si sarebbero altrimenti verificate. Ovviamente non si dovrebbe tener conto della collaborazione prestata dal titolare nella misura in cui questa sia prevista per legge, come ad esempio nel caso in cui consenta l'accesso ai locali per controlli o ispezioni.

g) **Le categorie di dati personali interessate dalla violazione**. L'autorità dovrà valutare se si tratta di categorie particolari dati quali quelli personali o quelli relativi a condanne penali, se i dati siano direttamente o indirettamente identificabili, se si tratta di dati la cui diffusione causerebbe danni o disagi immediati alla persona o, ancora, se i dati siano direttamente disponibili senza protezioni tecniche oppure siano criptati.

h) La maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione. Gli strumenti attraverso i quali l'autorità di controllo potrebbe venire a conoscenza della violazione sono i più disparati: indagini, reclami, articoli di giornale, suggerimenti anonimi oppure notifiche da parte del titolare del trattamento. Il titolare del trattamento ha l'obbligo a norma del regolamento di notificare all'autorità di controllo eventuali violazioni dei dati personali. Qualora questi si limiti ad adempiere a tale obbligo, la conformità ad esso non può essere interpretata come fattore attenuante. Analogamente, qualora il titolare ovvero il responsabile del trattamento abbiano agito incautamente senza notificare la violazione (o perlomeno senza notificarne tutti i dettagli) l'autorità di controllo potrebbe ritenere necessaria l'imposizione di una sanzione più grave, in quanto non in grado di valutarne adeguatamente la portata.

i) Qualora siano stati precedentemente disposti provvedimenti di cui all'art. 58 parag. 2[77] nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti. Il titolare del trattamento o il responsabile potrebbero già essere oggetto di attenzione dell'autorità di controllo per la verifica della conformità in seguito a una precedente violazione.

j) L'adesione ai codici di condotta approvati ai sensi dell'art. 40 o ai meccanismi di certificazione approvati ai sensi dell'art. 42. La non conformità con le misure di autoregolamentazione potrebbe rivelare la colpa o il dolo del titolare o del responsabile del trattamento.

k) Eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione. Le informazioni relative ai profitti derivanti da una violazione potrebbero risultare particolarmente importanti per le autorità di controllo in quanto il guadagno economico derivante dalla violazione non può essere compensato tramite misure che non abbiano una componente pecuniaria. Pertanto, il fatto che il titolare del trattamento abbia tratto profitto dalla violazione del regolamento può costituire una chiara indicazione della necessità di imporre una sanzione pecuniaria.

[77] Si tratta dell'applicazione dei poteri correttivi che fanno capo all'autorità di controllo.

GLOSSARIO

A

Accountability: principio di responsabilizzazione.

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

Attività principali: si devono considerare quelle che riguardano le attività primarie del Titolare e che esulano dal trattamento dei dati personali come attività accessoria. Le attività principali si possono, quindi, definire come quelle operazioni necessarie e che attraverso le quali il Titolare raggiunge i propri obiettivi. Tuttavia è bene ricordare che esse ricomprendono anche quelle in cui il trattamento dei dati costituisce una parte integrante dell'attività del Titolare. Le Linee Guida del WP29 chiariscono il concetto con un esempio: l'attività principale di un ospedale è quella di fornire assistenza sanitaria, ma questo non potrebbe raggiungere tale obiettivo in modo sicuro ed efficace senza elaborare i dati personali dei pazienti (che in questo caso sono dati sanitari e quindi appartenenti a quella particolare categoria di dati personali). Pertanto, l'elaborazione di questi dati deve essere considerata una delle attività principali dell'ospedale, con conseguente obbligo di designare un DPO.

Autorità di controllo: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

Autorità di controllo interessata: un'autorità di controllo interessata dal trattamento di dati personali in quanto il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure un reclamo è stato proposto a tale autorità di controllo;

C

Codici di condotta: codici elaborati dai titolari del trattamento o dai responsabili destinati a contribuire alla corretta applicazione del regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese. Tali codici possono essere elaborati anche dalle associazioni e dagli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento.

Consenso dell'interessato: 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 trattamento;

Contitolari del trattamento: due o più titolari che determinano congiuntamente, sulla base di un accordo interno, le finalità e i mezzi del trattamento.

D

Data breach: letteralmente "violazione dei dati personali". Una tale violazione deve essere notifica al Garante per la privacy e, in alcuni casi, anche ai soggetti interessati.

Dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

Dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

Dati personali: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

D.P.I.A.: Data Protection Impact Assessment. Acronimo inglese per indicare la valutazione di impatto sulla protezione dei dati.

D.P.O.: Data Protection Officer. Acronimo inglese per indicare il Responsabile della Protezione dei Dati Personali.

G

G.D.P.R.: General Data Protection Regulation. Acronimo inglese per indicare il Regolamento (UE) 2016/679.

Gestione dei rischi: insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi.

Gruppo imprenditoriale: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

I

Impresa: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

L

Limitazione di trattamento: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

N

Norme vincolanti d'impresa: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

O

Obiezione pertinente e motivata: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

Organizzazione internazionale: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

P

Privacy by default: letteralmente privacy "come impostazione predefinita". Questo implica che il titolare, nel trattare i dati personali raccolti, segua un percorso di politica aziendale o amministrativa interna che ne tuteli la diffusione non autorizzata.

Privacy by design: indica la necessità di tutelare il dato sin dalla progettazione di sistemi informatici che ne prevedano l'utilizzo. In altre parole, i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

Pseudonimizzazione: 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;

R

Rappresentante: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

Registro delle attività di trattamento: tenuto dal titolare del trattamento e, ove applicabile, dal suo rappresentante, contenente le seguenti informazioni: il nome e i dati di contatto del titolare del trattamento e, se presente, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati; le finalità del trattamento; la descrizione delle categorie di interessati e delle categorie di dati personali; le categorie di destinatari a cui i dati personali siano stati o saranno comunicati, compresi i destinatari di paesi terzi; i trasferimenti di dati personali verso paesi terzi e la loro identificazione (se presenti); i termini ultimi previsti per la cancellazione delle diverse categorie di dati; una descrizione generale delle misure di sicurezza tecniche e organizzative.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

Rischio: scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità.

S

Servizio della società dell'informazione: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio.

Stabilimento principale: ha due accezioni. Per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, si riferisce al luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale. Con riferimento, invece, a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

T

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

Trattamento su larga scala: secondo il Gruppo dei Garanti, al fine di verificare se si è o meno in presenza di un simile trattamento, devono considerarsi i seguenti fattori: numero di persone interessate, intese come numero specifico ovvero come percentuale della popolazione in questione; volume dei dati e/o la gamma di differenti unità di dati da elaborare; la durata o la permanenza dell'attività di elaborazione dei dati; l'estensione geografica dell'attività di trasformazione.

Trattamento transfrontaliero: è possibile fornire una duplice definizione. Può consistere nel trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il

responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure può consistere nel trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

V

Violazione dei dati personali: 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;