Segnalazione Novità Normativa
A cura di Antonio Musto e Luisa Piccolo

Noi pensiamo di discutere soltanto di protezione dei dati,
ma in realtà ci occupiamo del destino delle nostre società,
del loro presente e soprattutto del loro futuro (S. Rodotà[1])**.**

Le maggiori novità di interesse notarile apportate dal nuovo regolamento *privacy* europeo

Abstract

L'obiettivo della presente segnalazione è quello di fornire un primo inquadramento teorico del Regolamento europeo sulla protezione dei dati personali delle persone fisiche n. 679/2016, cd General Data Protection Regulation *(G.D.P.R.), in vigore nei Paesi dell'Unione Europea a partire dal 25 maggio 2018.*

Il G.D.P.R., inserendosi nel solco iniziato dalla nota "Direttiva madre" (dir. 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995), si propone come uno strumento di uniformazione della materia relativa alla protezione dei dati personali, nonostante non manchino anche incisivi rinvii alle legislazioni nazionali.

In questa prospettiva, nell'offrire un'istantanea argomentativa del Regolamento, si rileverà come alcune disposizioni non hanno un contenuto propriamente innovativo rispetto all'esperienza italiana; altre sono nuove, invece, come quella sui dati biometrici e quella in tema di pseudonimizzazione; in altre, ancora, sono state aggiunte delle precisazioni, come con riferimento all'informativa. In parte nuova, certamente di grande rilevanza, è la disciplina sul trasferimento dei dati all'estero. Sono stati inoltre previsti alcuni meccanismi per garantire un'applicazione uniforme del Regolamento nell'Unione europea, attraverso il c.d. "meccanismo di coerenza". Mutano le disposizioni sul foro competente, con le previsioni di più fori alternativi, nonché il regime di responsabilità civile. Sono molto elevate le sanzioni amministrative previste, le quali possono giungere sino al 4% del fatturato, rendendo così la nuova disciplina in materia di protezione dei dati personali ben più efficace dell'attuale.

*Permea l'intero Regolamento il cd "*risk-based approach"*, ossia un approccio basato sul rischio, in cui ai soggetti che effettuano il trattamento dei dati personali si richiede di valutare l'effettivo grado di rischio che le attività caratteristiche del titolare presentano per i diritti e le libertà individuali, effettuando la cd valutazione di impatto prima di procedere al trattamento.*

Se quella sin qui descritta, sia pure succintamente, è la struttura del Regolamento, ai nostri fini, s'impone una trattazione dello stesso nella prospettiva del pubblico ministero esercitato dal Notaio, al quale sovente occorre di trattare dati personali al fine di osservare i diversi adempimenti impostigli dalla legge. Così, a titolo esemplificativo, da un canto, potrebbero individuarsi delle aree - come la profilazione dei dati - che non ineriscono direttamente all'attività notarile; d'altro canto, dovrebbero analizzarsi le tematiche delle condizioni di liceità del trattamento dei dati personali e dei diritti dell'interessato.

Guida dell'interprete, nell'auspicata prospettiva ermeneutica, sono i principi e i valori contenuti nella disciplina del Regolamento, dove lo stesso diritto alla protezione dei dati personali è inteso, non già in maniera assoluta, bensì alla stregua di un diritto necessariamente oggetto di un ragionevole bilanciamento con altri diritti fondamentali nonché con i principi sanciti dalla Carta dei diritti fondamentali dell'Unione europea, nel rispetto del principio di proporzionalità e della sua funzione sociale.

[1] Parole mirifiche, di tensione ideale diacronica, oltre la sola dimensione giuridica, S. RODOTÀ, Privacy, *libertà, dignità, Discorso conclusivo della Conferenza internazionale sulla protezione dei dati*, 26a Conferenza Internazionale sulla Privacy e sulla Protezione dei Dati Personali Wroclaw (PL), 14, 15, 16 settembre 2004. «Di più: ciò che più preme a Rodotà è proprio la crescente domanda che si rivolge al diritto di regolare momenti e aspetti vitali che dovrebbero essere lasciati alla personale decisione dei singoli, al loro modo di concepirsi nel loro rapporto con gli altri. Dunque, una nuova rivendicazione della storicità del diritto, basata sull'autorità dei diritti», così, G. ZACCARIA, *Interpretazione e metodo nelle prolusioni raccolte*, in *Contr. e impr*., 2016, 45.

Sommario: 1. Premessa. **2**. Ambito applicativo materiale e territoriale. **3.** Dati personali: nozione e categorie. **4.** Il trattamento dei dati personali: principi, condizioni di liceità e sanzioni previste. **5.** Diritti dell'interessato: definizione e catalogazione da parte dei primi commentatori. **5.1**. Diritto all'informativa. **5.2.** Diritto di accesso. **5.3.** Diritto di conferma del trattamento. **5.4.** Diritto alla comunicazione di una violazione dei dati. **5.5.** Diritto alla limitazione del trattamento. **5.6.** Diritto di opporsi. **5.7.** Diritto alla portabilità dei dati**. 5.8.** Diritto alla rettifica/integrazione dei dati inesatti. **5.9**. Diritto alla cancellazione. **5.10.** Diritto all'oblio. **6**. Le figure coinvolte dal trattamento dei dati personali. **6.1.** L'interessato dal trattamento. **6.2.** Il Titolare e il contitolare del trattamento. **6.3.** Il Responsabile del trattamento e il Rappresentante del titolare e del responsabile del trattamento. **6.4.** Il Responsabile della protezione dati (DPO). **7.** Rischio e responsabilizzazione. **7.1**. *Accountability*. **7.2.** *Privacy by design* e *by default*. **7.3**. *Data breach notification*. **7.4.** *Data protection impact assessment*. **8.** Il Registro generale delle attività di trattamento svolte sul dato personale del trattato. **9.** I codici di condotta e le certificazioni **10.** I poteri delle Autorità di controllo.

1. Premessa.

Il presente contributo intende offrire un primo inquadramento teorico del Regolamento europeo sulla protezione dei dati personali delle persone fisiche n. 679/2016, cd *General Data Protection Regulation* (G.D.P.R.), pubblicato sulla Gazzetta Ufficiale dell'Unione europea del 4 maggio 2016 e in vigore nei Paesi dell'Unione Europea a partire dal 25 maggio 2018[2].

Il G.D.P.R. s'inserisce nel percorso iniziato quattro lustri or sono dalla cd "*Direttiva madre*" (dir. 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995)[3]. Esso si propone come una risposta alle nuove sfide che la globalizzazione e la rapidità dell'evoluzione tecnologica comportano per la protezione dei dati personali (cfr. considerando n. 6)[4], nonché come un rimedio all'attuale frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione. A tal fine raccoglie, con diversi arricchimenti e specificazioni, l'elaborazione europea in materia di

[2] La bibliografia sul tema è vasta. Per una diffusa e approfondita trattazione, maggiormente, AA.VV., *Il nuovo Regolamento europeo sulla* privacy *e sulla protezione dei dati personali*, diretto da Giu. Finocchiaro, Bologna, 2017; AA.VV., *La nuova disciplina europea della* privacy, a cura di Sica, D'Antonio e G.M. Riccio, Milano, 2016; L. BOLOGNINI-E. PELINO-C. BISTOLFI, *Il Regolamento* Privacy *europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016; F. PIZZETTI, Privacy *e il diritto europeo alla protezione dei dati personali*, I (*Dalla dir. 95/46 al nuovo regolamento europeo*) e II (*Il regolamento europeo 2016/679*), Torino, 2016; E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contr. e impr*., 2018; M.G. STANZIONE, *Il regolamento europeo sulla* privacy*: origini e ambito di applicazione*, in *Eur. dir. priv.*, 2016, p. 1249 ss.; S. THOBANI, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Eur. dir. priv*, 2016, p. 513 ss.; F. PIRAINO, *Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ. comm*., 2017, 394; A. THIENE, *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo regolamento europeo*, *ivi*, 2017, 2, 410. Per un taglio teorico-applicativo, con schede a confronto di diversi Autori e quadri sinottici di orientamento, cfr. anche GDPR, a cura di *Bird & Bird-Gattai Minoli Agostinelli & Partner*, in *InPraticaLegale*, in *http://www.inpratica.leggiditalia.it*, da dove utili spunti, ai fini della presente segnalazione, pure sono stati evinti.

[3] Cfr. G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, in *Nuove Leggi civ. Comm*., 2017, 1, 1.

[4] Sfida intrapresa anni addietro, con considerevole lungimiranza e rigore accademico, da S. RODOTÀ, di cui cfr., in particolare, Privacy, *libertà, dignità*, discorso conclusivo della Conferenza internazionale sulla protezione dei dati, tenuto alla ventiseiesima Conferenza Internazionale sulla Privacy e sulla Protezione dei Dati Personali (Wroclaw (PL), 14, 15, 16 settembre 2004), dove ha sottolineato in particolar modo il rapporto tra *privacy*, libertà e dignità, affermando: «Nel quadro della *privacy*, la dignità si precisa come un concetto riassuntivo dei principi di riconoscimento della personalità e di non riduzione a merce della persona, di eguaglianza, di rispetto degli altri, di eguaglianza, di solidarietà, di non interferenza nelle scelte di vita, di possibilità di agire liberamente nella sfera pubblica. Ad essa è estranea la pretesa di imporre valori. Non si impongono valori. Si pongono le premesse per l'autonomia ed il rispetto reciproco».

privacy[5] e si presenta alla stregua di una *Magna Charta* della circolazione dei dati personali e della protezione della persona[6].

Il legislatore europeo, ricorrendo alla fonte regolamentare[7], ha prescelto uno **strumento di uniformazione**, sebbene non manchino incisivi rinvii ai legislatori nazionali[8], specie con riferimento al trattamento dei dati personali per l'adempimento di un obbligo legale e per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, nonché in ordine al trattamento di categorie particolari di dati personali(cfr. il Considerando n. 10). A tal proposito si segnala che, nel momento in cui si scrive, è in corso di approvazione il decreto legislativo di armonizzazione del d.lgs. 30 giugno 2003, n. 196 (cd *codice privacy*) con il G.D.P.R.[9].

Nell'offrire **un'istantanea del Regolamento**, può rilevarsi che alcune disposizioni non hanno un contenuto innovativo rispetto all'esperienza italiana; altre disposizioni sono invece nuove, come quella sui dati biometrici e quella relativa alla pseudonimizzazione. In altre sono state aggiunte delle precisazioni, come con riferimento all'informativa. Ancora, è stato inserito un articolo *ad hoc* sul consenso dei minori[10]. Sono stati dettagliatamente disciplinati alcuni diritti, quali il diritto alla cancellazione dei dati; mentre altri sono stati introdotti, come quello alla portabilità dei dati, ossia il diritto di trasferire i propri dati da un sistema di trattamento elettronico ad un altro. In parte nuova, certamente di grande rilevanza, è la disciplina (contenuta nei Considerando 6-101-102-115 e negli artt. 44 ss.; 83, paragrafo 5, lett. c); 96 del Regolamento) sul trasferimento dei dati all'estero, per «assicurare una libera circolazione dei dati personali per garantire l'incremento della economia europea in un mondo sempre più connesso, coniugandola però con la necessaria tutela dei diritti degli interessati»[11]. Sono stati previsti inoltre alcuni meccanismi per garantire un'applicazione uniforme del Regolamento nell'Unione europea, attraverso il c.d. "*meccanismo di coerenza*". Molto elevate le sanzioni amministrative che possono giungere fino al 4% del fatturato, rendendo così la nuova disciplina in materia di protezione dei dati personali ben più efficace dell'attuale[12].

---

[5] Cfr. G. FINOCCHIARO, *op.cit.*, §4, secondo la quale il Regolamento raccoglie l'esperienza maturata in Europa negli ultimi venti anni e cerca di riordinare e razionalizzare la frammentaria disciplina esistente sulla protezione dei dati personali nell'Unione europea, tanto che in dottrina è stato accostato alla figura del testo Unico.

[6] Così si è espresso F. PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civili e commentate*, 2/2017, 394.

[7] Si è osservato in dottrina come l'utilizzo di un regolamento, in luogo della direttiva, sia significativo del mutamento di approccio da parte del legislatore europeo, il quale ha avvertito la necessità di sostituire l'obiettivo originario dell'armonizzazione con quello assai più pervasivo e ambizioso dell'uniformazione: cfr. A. IULIANI, *Note minime in tema di trattamento dei dati personali*, in *Europa e Diritto Privato*,1, 293,ss., § 3; G. FINOCCHIARO, *Introduzione al Regolamento europeo sulla protezione dei dati*, *Nuove leggi civ. comm*., 2017, § 3.

[8] Così vd. A. IULIANI, *op.cit.*, § 3.

[9] Nell'ultima versione nota del testo del decreto legislativo, in luogo di un'abrogazione totale del decreto legislativo 196 del 2003 (scelta iniziale del legislatore), si procede ad un'armonizzazione delle norme italiane con il contenuto del GDPR, con una abrogazione selettiva e s'introducono una serie di sanzioni penali.

[10] «La vera novità riguarda invece il regolamento il riconoscimento in capo al minore di età di almeno sedici anni di centro di imputazione giuridica del diritto alla protezione dei dati personali, il minore ultrasedicenne diviene pertanto titolare di tale diritto e potrà rilasciare un valido consenso per i servizi relativi alla società dell'informazione e pertanto i servizi erogati in forma digitali su *internet* (articolo 8 del regolamento europeo)» F. DI RESTA, *La nuova privacy europea*, Torino, 2018, 72. A completamento della disciplina, cfr. Considerando 38, in dottrina G. SPOTO, *Disciplina del consenso e tuela del minore*, in *La nuova disciplina europea della privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Padova, 2016, 110 ss., spec. 121, dove si segnala il passaggio dal dovere di ascolto all'autodeterminazione. Per prassi "*Guidelines on Consent under Regulation 2016/679*", p. 25.

[11] F. FIORE-G. LIPARI, *Il trasferimento dei dati all'estero (artt. 44-50)*, in *Adempimenti privacy per professionisti e aziende*, C. CARDARELLLO-F. D'AMORA-F. FIORE, Milano, 2018, 149. Sul tema, D. PITTELLA, *Trasferimento verso paesi terzi*, in *La nuova disciplina europea della privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Padova, 2016, 259.

[12] Per questo efficace quadro di sintesi cfr. G. FINOCCHIARO, *op.cit.*, § 4.

L'intero Regolamento si fonda sull'accolto principio del cd "*risk-based approach*", letteralmente c.d. "approccio basato sul rischio"[13], in base al quale i soggetti che effettuano il trattamento dei dati personali devono valutare l'effettivo grado di rischio che le attività caratteristiche del titolare presentano per i diritti e le libertà individuali, effettuando la cd **valutazione di impatto** prima di procedere al trattamento[14].

Se quella sin qui descritta, sia pure succintamente, è la struttura del Regolamento[15], ai nostri fini s'impone una trattazione dello stesso nella prospettiva del pubblico ministero esercitato dal Notaio, al quale sovente occorre di trattare dati personali al fine di osservare i diversi adempimenti impostigli dalla legge.

In tale direzione, a titolo esemplificativo, da un canto, potrebbero individuarsi delle aree - come la profilazione dei dati - che non ineriscono direttamente all'attività notarile; d'altro canto, dovrebbero analizzarsi le tematiche delle condizioni di liceità del trattamento dei dati personali e dei diritti dell'interessato.

In merito al primo profilo, di là dalle ipotesi in cui vi è il consenso dell'interessato, sembrerebbero poter assumere rilievo le condizioni di liceità indicate dall'art. 6 del Regolamento, secondo cui è lecito il trattamento ove necessario:

- per adempiere un obbligo legale cui è soggetto il titolare del trattamento (lettera c);

- per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (lettera e).

Allo stesso modo, nella valutazione della liceità del trattamento di dati particolari sembrerebbe vengano in rilievo le disposizioni dell'art. 9 secondo cui il trattamento:

- riguarda dati personali resi manifestamente pubblici dall'interessato (lettera e): si pensi al riguardo ai dati confluiti in pubblici registri;

- è necessario per la difesa in giudizio del diritto (lettera f): basti ricordare al riguardo che l'atto pubblico costituisce prova legale ai sensi dell'art. 2700 c.c.;

---

[13] Sottolinea, fra gli altri, questo profilo, G. GIANNONE CODIGLIONE, Risk-based approch *e trattamento dei dati personali*, in *La nuova disciplina europea della privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Padova, 2016, 55. Cfr. anche, M. SOFFIENTINI, *Nuovi comportamenti per la compliance aziendale della privacy*, in *Dir. e Pratica Lav*., 2017, 41, il quale rileva come «L'introduzione del c.d. "approccio basato sul rischio" (*Risk based approach*) e, più in generale del principio di *accountability*, ovvero di responsabilizzazione dei titolari di trattamento obbligherà soggetti privati e pubblici, ciascuno nell'ambito dei propri diritti e doveri, a sviluppare sistemi di gestione *privacy* capaci di prevenire possibili problematiche. L'applicazione dei principi di *privacy by design* e *privacy by default*, nonché l'obbligo in molti casi di condurre una valutazione di impatto *privacy* prima di procedere ad un trattamento, saranno alcuni tra i principali strumenti a disposizione del titolare del trattamento per contenere la responsabilità giuridica ascrivibile alla sua condotta in tema di *data protection*».

[14] In altri termini «il titolare è tenuto a valutare le proprie attività di trattamento in ottica *risk based*, in maniera tale da indirizzare coerentemente le proprie scelte tecniche ed organizzative. Tuttavia, sono presenti nel dettato normativo anche degli specifici obblighi ed adempimenti che devono essere curati in ogni caso» M. GAGLIARDI, *Gli adempimenti previsti dal Regolamento: quadro generale, i registri*, in *Manuale per il trattamento dei dati personali*, a cura di G. COMANDÈ e G. MALGIERI, Milano, 2018, 63 ss.

[15] Come evidenziato, con attenzione, in dottrina «La disciplina del trattamento dei dati personali appare divisa in due grandi blocchi, seppur tra di essi comunicanti: in primo luogo si rinvengono le attività di trattamento di "prima generazione", riferite ad un'accezione qualitativa di dato personale. (…). Dall'altra parte si staglia una differente tipologia di attività, collegata alla prima sotto il profilo della fonte di legittimazione e delle regole generali, ma riferibile ad una nozione di tipo quantitativo di dato personale e relativa ad attività di accumulo e combinazione secondaria dei dati previamente raccolti» G. GIANNONE CODIGLIONE, Risk-based approch *e trattamento dei dati personali*, in *La nuova disciplina europea della privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Padova, 2016, 74 s.

- è necessario per motivi di interesse pubblico rilevante, sulla base del diritto dell'Unione o degli Stati Membri (lettera g).

In merito al secondo profilo, sembrerebbe che, la cristallizzazione dei dati in un atto pubblico, osti al riconoscimento *sic et simpliciter* dei diritti dell'interessato inerenti alla rettifica, nonché all'integrazione, non riconducibile ad errori relativi a dati preesistenti alla sua redazione.

In questo scenario, guida dell'interprete, nell'auspicata prospettiva ermeneutica, sono i principi e i valori contenuti nella disciplina del Regolamento, dove lo stesso diritto alla protezione dei dati personali è inteso, non già in maniera assoluta, bensì alla stregua di un diritto necessariamente oggetto di un ragionevole bilanciamento con altri diritti fondamentali nonché con i principi sanciti dalla Carta dei diritti fondamentali dell'Unione europea[16], nel rispetto del principio di proporzionalità e della sua funzione sociale (cfr. considerando n. 4)[17].

2. Ambito applicativo materiale e territoriale.

Gli artt. 2 e 3 del Regolamento definiscono rispettivamente l'ambito di applicazione materiale e territoriale.

Dal punto di vista materiale, il Regolamento si applica «*al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi*» (cfr. l'art. 2, primo comma).

Non si applica, per espresso dettato normativo (cfr. l'art. 2, secondo comma), al trattamento di dati personali effettuati:

a) per **attività che non rientrano nell'ambito di applicazione del diritto dell'Unione**[18];
b) dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE, *id est* le attività riguardanti la **Politica estera e Sicurezza Comune;**
c) da una persona fisica per l'esercizio di **attività a carattere esclusivamente personale o domestico**[19];

[16] Come prontamente ha osservato G. FINOCCHIARO, *op. cit.*, § 5.4, il considerando n. 4 «riporta alla mente alcune affermazioni della Corte di Cassazione italiana, in particolare quella contenuta nella sentenza n. 10280/2015 della Sezione III della Corte di Cassazione, ove si afferma che il diritto alla protezione dei dati personali, qualificato come pretesa ad esigere una corretta gestione dei propri dati personali, pur rientrando nei diritti fondamentali della persona, non è un "*totem* al quale possano sacrificarsi altri diritti altrettanto rilevanti sul piano costituzionale e, conseguentemente, la disciplina in materia va coordinata e bilanciata da un lato con le norme che tutelano altri e prevalenti diritti (tra questi, l'interesse pubblico alla celerità, trasparenza ed efficacia all'attività amministrativa); dall'altro, con le norme civilistiche in tema di negozi giuridici"». Cfr. sul punto anche la successiva Cass., 17 luglio 2015, n. 15096, in *www.deiure.it*.

[17] In dottrina cfr. A. RICCI, *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, in *Contratto e Impr*., 2017,2, 586 la quale analizza il significato della norma e dell'affermazione ivi contenuta sulla «non assolutezza» del diritto alla protezione dei dati personali, soffermandosi altresì sul senso da attribuire al richiamo alla «funzione sociale».

[18] Ciò comporta - secondo C. CARDARELLO, in AAVV, *Adempimenti privacy per professionisti e aziende*, a Milano, 2018, 12 - che ciascuno Stato membro avrà facoltà di legiferare e regolarsi autonomamente.

[19] Tanto dovrebbe escludere, secondo parte della dottrina, l'applicazione del regolamento al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività in cui non vi sia una connessione con un'attività commerciale o professionale e che gli stessi trattamenti per scopi personali riguardano la corrispondenza e gli indirizzari, o la socializzazione in rete e attività in linea intraprese nell'ambito di tali attività a carattere personale o domestico; C. CARDARELLO, 13. L'A. rileva che il regolamento non precisa se si applicherà a trattamenti di dati personali per scopi personali destinati ad una diffusione o ad una comunicazione sistematica (così come prevede il Codice della *privacy*, dlgs 196/2003). Secondo l'A. peraltro, l'esclusione dall'ambito applicativo materiale del regolamento non significa esclusione di qualsiasi regolamentazione normativa: trovano applicazione le tutele

d) 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.

Infine sono previste due riserve:

- si applica il regolamento CE n. 45/2001 al **trattamento dei dati personali da parte di istituzioni organi, uffici e agenzie dell'Unione**[20];
- il Regolamento non pregiudica l'applicazione della **direttiva 2000 /31/CE**, in particolare le norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli articoli da 12 a 15 della medesima direttiva.

Dal punto di vista territoriale, il Regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di **uno stabilimento** da parte di un titolare del trattamento o di un responsabile del trattamento dell'Unione europea, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione (cfr. art. 3, comma 1). Su questo profilo, il *Considerando* n. 22 precisa che «lo **stabilimento** implica l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile» e che a tal riguardo «non è determinante la forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica»[21].

Si è osservato che il regolamento «**supera il principio della territorialità in senso stretto[22] e modifica la concezione tradizionale del principio di stabilimento»[23].** La disciplina ivi recata trova così applicazione (giusta l'art. 3, comma2) anche rispetto al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che **non è stabilito nell'Unione**, quando le attività di trattamento riguardano:

a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato[24];

---

civilistiche e penalistiche dell'individuo (l'A. reca gli esempi delle tutele previste in materia di diffamazione, tutela dell'immagine).

[20] Sul punto è specificamente previsto dal comma 3 dell'art. 2 che il regolamento (CE) n. 45/2001 e gli altri atti giuridici dell'Unione applicabili a tale trattamento di dati personali devono essere adeguati ai principi e alle norme del regolamento conformemente all'articolo 98.

[21] Per "stabilimento principale", secondo l' art. 4, comma 1, n. 16 s'intende: «a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, 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 riferimento 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».

[22] In dottrina, G. FINOCCHIARO, *op. cit.*, § 5.3, osserva come in tal senso militasse anche la giurisprudenza della Corte di Giustizia europea con molte decisioni, fra le quali le più note: quelle relative ai casi *Google e Schrems* (sul punto cfr., anche per i richiami, della stessa Autrice, in AA.VV., L*a protezione transnazionale dei dati personali dai "safe harbour principles"al "privacy shield"*, RESTA-ZENO ZENCOVICH (a cura di), Roma, 2016.

[23] Sull'evoluzione della nozione di stabilimento cfr., anche per i richiami, M.G. STANZIONE, *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Europa e diritto privato*, 4, 2016, 1249 ss., § 2. *Adde* su questa norma anche F. DI RESTA, *op.cit.*, 28, il quale rimarca come essa rappresenti una disposizione con intento universalistico nel diritto europeo molto importante anche da uun punto di vista politico e diplomatico

[24] Sul punto, M.G. STANZIONE, *op.cit.*, § 2, osserva che tale criterio sia corrispondente all'elaborazione della giurisprudenza della Corte di Giustizia dell'Unione Europea per cui le nuove questione interpretative si porranno con

b) oppure il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione[25].

I *Considerando* 23 e 24 recano dei parametri per stabilire quando si possa ritenere sussistente una offerta di beni/servizi o un monitoraggio del comportamento degli interessati.

In dettaglio, non costituiscono indici della volontà del titolare o responsabile del trattamento di offrire beni o servizi agli interessati che si trovano nell'Unione fattori quali la semplice accessibilità del sito web del titolare del trattamento, del responsabile del trattamento o di un intermediario nell'Unione, di un indirizzo di posta elettronica o di altre coordinate di contatto o l'impiego di una lingua abitualmente utilizzata nel paese terzo in cui il titolare del trattamento è stabilito. Al contrario, possono evidenziare l'intenzione del titolare o del responsabile del trattamento di offrire beni o servizi agli interessati nell'Unione 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 la menzione di clienti o utenti che si trovano nell'Unione possono (cfr. il *Considerando* n. 23).

Per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche siano 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 (cfr. il *Considerando* n. 24).

Infine, il Regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico (cfr. art. 3, comma 3). Su quest'ultimo profilo, il *Considerando* n. 25 propone l'esempio della rappresentanza consolare o diplomatica di uno Stato membro quale luogo soggetto al diritto di quello Stato in cui operi l'eventuale titolare non stabilito nell'Unione.

3. Dati personali: nozione e categorie.

Il Regolamento definisce la nozione di dato personale[26] quale «*qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato*")» e precisa che «*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*

riferimento agli elementi probanti l'esistenza di un'offerta di beni o servizi, a prescindere dalla sussistenza di un'obbligazione di pagamento dell'interessato.

[25] Sul punto, M.G. STANZIONE, *op.cit.*, § 2, osserva che si assiste ad una significativa innovazione dal momento che le risposte all'interrogativo sull'applicabilità della disciplina europea si legano all'interpretazione della nozione di monitoraggio del comportamento degli utenti e alla sua variabilità e apre an ora più le frontiere dell'applicazione del diritto dell'Unione in materia di protezione ei dati personali.

[26] In dottrina si è puntualizzato che «Il dato personale rappresenta uno strumento tecnico giuridico attraverso il quale sia il legislatore europeo che quello italiano hanno scelto di tutelare quell'insieme di diritti collegati all'identità personale, alla riservatezza, al diritto alla protezione dei dati personali. Il dato è perciò un contenitore vuoto all'interno del quale l'interprete inserisce di volta in volta uno specifico contenuto relativo al patrimonio informativo dell'interessato»: così F. DI RESTA, *La nuova privacy europea*, Torino, 2018, 3-4, il quale si sofferma sulla nozione di dato personale di cui al codice della privacy e sulla relativa evoluzione nel contesto sociale.

relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale»[27]..

Questa definizione del legislatore europeo conferma la nozione presente nel codice *privacy*, ma indica in modo espresso che anche i dati di ubicazione e quindi di geolocalizzazione sono dati personali analogamente ai dati biometrici, genetici, psichici, economici, culturali e sociali[28].

La terminologia usata, nella sua nettezza e semplicità, comporta una nozione amplissima di dato personale, coerente con la volontà del legislatore di estendere al massimo la tutela di questo diritto[29].

---

[27] In dottrina G. MALGIERI, in *Manuale per il trattamento dei dati personali*, G. COMANDÈ e G. MALGIERI, Milano, 2018, 70, 7, osserva che «nonostante l'elencazione degli "identificativi" possa aiutare a stabilire se una persona a cui si riferiscono alcuni dati si possa considerare "identificabile", la loro ampiezza e vaghezza (es. "elementi caratteristici dell'identità economica, culturale, sociale") lascia aperto il problema della concreta identificabilità dei soggetti: cosa si intende per elementi "caratteristici dell'identità? È sufficiente la presenza di un solo identificativo affinché un soggetto sia "identificabile"? e dunque, ogni tipo identificativo ha lo stesso valore?». Come l'Autore in discorso adduce, per rispondere a questi quesiti soccorre il considerando 26 del Regolamento, secondo cui «*Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca*». Ne discende - come conclude l'Autore richiamato - che l'identificabilità di un soggetto è un concetto relativo, che va valutato caso per caso, variabile nel tempo.

Sulla nozione di identità personale e la sua evoluzione nel corso del tempo cfr., autorevolmente, G. ALPA, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contratto e impr*., 2017, 723, il quale evidenzia come, mentre in passato l'identità (della persona) era conchiusa nella sua consistenza fisica ed affidata ad alcuni riferimenti precisi, tendenzialmente immodificabili, burocraticamente registrabili, dalla metà del Novecento in poi è stata oggetto di una elaborata costruzione giuridica i cui fattori propulsivi sono strettamente connessi con una maggiore attenzione degli ordinamenti giuridici dei Paesi occidentali ai valori stessi della persona; così – rileva l'Autore - all'identità fisica si è affiancata l'identità ideale, che, nel nostro ordinamento, ha preso il nome tecnico di diritto alla identità personale. Sagacemente, tale dottrina, considerata l'evoluzione della tecnica e delle biotecnologie, osserva che «L'identità non è un concetto statico, ma dinamico, come lo è la identità fisica, che ne costituisce la matrice. Se si pensa alla collocazione dell'identità nel tempo, ci si avvede della sua trasformazione per cause naturali o per interventi volontari o accidentali. E non solo l'aspetto fisico muta, muta il rapporto con i luoghi, cambiano anche i rapporti familiari, le occupazioni, le credenze, le adesioni partitiche e filosofiche. La persona si è così vista riflessa in mille diverse raffigurazioni, come accade quando ci si pone di fronte ad uno specchio frantumato, in cui ciascun frammento riflette una parte, un aspetto, uno spicchio dell'oggetto che gli si pone dinnanzi (…). L'identità personale non è più soltanto un modo di essere e di rappresentare la persona considerata individualmente, ma è diventato un problema sociale e, nel mondo conflittuale di oggi, anche una ragione di conflitto, di atrocità, di migrazione, quando è associata ad una Nazione, ad una religione, ad una minoranza linguistica, ad una etnia. L'identità è diventata un concetto liquido. E il diritto alla identità un diritto connesso con una realtà fattuale fluttuante, dinamica, fluida, quasi inafferrabile».

[28] Così F. DI RESTA, *op.cit.*, 6.

[29] Così F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali, Dalla direttiva 95/46 al nuovo Regolamento europeo*, I, Torino, 2016, 184. Sull'ampia nozione di dato personale *adde* G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, § 2, secondo cui «muovendo (…) dall'ampia definizione di dato personale, il diritto alla protezione dei dati personali si configura come il diritto di un soggetto di controllare l'insieme delle informazioni che a questi si riferiscono e che quindi costituiscono il suo riflesso e delineano lo stesso suo essere nella società dell'informazione» (sul punto l'Autrice richiama S. RODOTÀ, allora Presidente dell'Autorità Garante per la protezione dei dati personali, sulla nozione di "corpo elettronico", nella Relazione 2002 sull'attività dell'Autorità Garante per la protezione dei dati personali, Roma, Presidenza del Consiglio dei Ministri, 20 maggio 2003; nonché l'opera dello stesso A., *Tecnologie e diritti*, Bologna, 1995); *adde* ancora M. GRANIERI, *Il trattamento di categorie particolari di dati personali nel reg. ue 2016/679*, in *Nuove leggi civ. comm*., 2017, 1, 165 il quale puntualizza che «dovrebbero dunque ritenersi sciolti i dubbi di quella parte della dottrina che si interrogava circa la inclusione dei cd. *R-*

Si specifica che il dato personale è costituito da quattro elementi:

1. l'informazione (ossia il contenuto del dato);
2. la persona fisica, ossia il soggetto a cui il contenuto viene collegato;
3. il collegamento, ossia l'operazione logica che correla la persona fisica al contenuto del dato;
4. l'identificazione / identificabilità della persona fisica (altrimenti si avrebbe un'informazione anonima)[30].

L'identificazione/identificabilità è un requisito essenziale della nozione di dato personale. Ove risultasse impossibile o venisse meno in modo definitivo, bisognerebbe parlare di **informazione anonima o anonimizzata**, mancherebbe un soggetto determinato a cui riferire il contenuto informativo. Va anche notato che se vi è identificazione / identificabilità vi è necessariamente anche un identificativo, ossia un elemento presente nel dato personale che permette il processo di identificazione[31].

Secondo una consolidata impostazione, ai fini dell'identificazione, non è necessaria la determinazione del nome anagrafico della persona fisica, ma è sufficiente l'individuazione della persona all'interno di un contesto, a prescindere dalla conoscenza del nome. Ne deriva l'**equipollenza**, ai fini della nozione di dato personale, **tra il nome anagrafico e qualsiasi altro elemento informativo o complesso di elementi informativi ugualmente dotati di attitudine distintiva** (cfr. in tal senso anche il *Considerando* n. 26).

Peraltro, alcuni identificativi non sono univoci, ma hanno attitudine distintiva solo in relazione ad alcuni contesti: «ai fini della qualificazione di una informazione come dato personale non rileva che la persona fisica sia individuabile da chiunque, ciò che conta è che possa essere distinta o riconosciuta con ragionevole probabilità almeno da qualcuno, ad esempio entro una cerchia di persone che frequenta o da quella costituita dai suoi familiari…ciò è ritenuto assolutamente sufficiente ai fini della nozione di "dato personale" e determina l'applicazione delle tutele riconosciute dal Regolamento»[32]. Ciò nonostante il concetto di **dato personale è assoluto**, non relativo: «un'informazione o è dato personale oppure non lo è. Una volta che essa è qualificata come "dato personale", in un qualunque contesto, lo è in ogni altro. Questo implica che il titolare del trattamento potrebbe in concreto anche non conoscere l'identità dell'interessato né avere ragionevolmente modo di determinarla (come nel caso in cui il titolare abbia acquisito da altro titolare l'informazione). Nondimeno, anche in tal caso, il trattamento riguarderà dati personali e non informazioni anonime»[33].

---

identifiers (*recognition identifiers*) e il superamento degli *L-identifiers* (*lookup identifiers*)». Nondimeno l'Autore non manca di osservare che, sebbene la formula possa ora consentire di riferirsi al dato nella maniera più inclusiva e onnicomprensiva, l'ampiamento della nozione di dato personale e la sua declinazione come dato che rientra nelle categorie particolari non rappresentano di per sé soli elementi di maggiore tutela, perché paradossalmente la dilatazione di ciò che si intende per dato personale aumenta, anziché diminuire, le difficoltà di effettiva tutela in tutti i contesti di emersione delle informazioni personali.

[30] Così E. PELINO, in BISTOLFI, BOLOGNINI, PELINO, *Il Regolamento privacy europeo, Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, 43 ss. il quale evidenzia come le nozioni di informazioni e di collegamento presentino un elevato coefficiente di astrazione e flessibilità. Ne deriva che la nozione di dato personale risulta particolarmente ampia sul piano applicativo. Alla base si ravvisa una precisa scelta del legislatore europeo, che non ha ritenuto opportuno esporre a pericolo le garanzie dell'interessato costruendo un concetto facilmente limitabile (vd. p. 47). Similmente cfr. F. DI RESTA, *op.cit.*, 8, il quale suddivide nei seguenti quattro punti la definizione di dato personale: 1. qualsiasi informazione; 2. concernente l'interessato a cui si riferiscono i dati; 3. identificata o identificabile (riferito all'informazione), 4. (Persona fisica, riferito all'interessato).

[31] E. PELINO, *op.cit*., 50 - 51

[32] Così E. PELINO, *op.cit.*, 52-53.

[33] Così E. PELINO, *op.cit.*, 52-53.

Un dato personale può essere collegato a più soggetti (**dato pluripersonale**), dunque presentare una pluralità di interessati. Si tratta di una situazione complessa, non infrequente, nella quale si pone il problema concreto di definire rapporti di prevalenza tra pretese potenzialmente confliggenti tra i cointeressati (si pensi all'esercizio del diritto di accesso rispetto a dati che sono anche riferibili ad altro controinteressato, come il cointestatario di un conto corrente bancario). In dottrina si ritiene possibile, alla luce dell'impostazione consolidata del Garante, l'esercizio del diritto di accesso rispetto a dati plurisoggettivi, quando questi siano inestricabilmente connessi, ossia quando i dati personali relativi al richiedente (ed eventuali altre notizie o informazioni inerenti a terzi) siano intrecciati al punto tale da rendere i primi non comprensibili, oppure snaturati nel loro contenuto, se privati di alcuni elementi essenziali per la loro comprensione, tra i quali possono rientrare informazioni relative a cointestatari che effettuino operazioni rilevanti nel comune rapporto[34].

Si distingue altresì tra **dati oggettivi** e i **dati soggettivi o valutativi**. Esempi del primo tipo sono costituiti dalle generalità di una persona, dalle coordinate di contatto, dalle caratteristiche fisiche, dall'immagine, dalla voce, dalle informazioni sulla localizzazione, sulle relazioni sociali o, ancora, sulle scelte che manifesta. Informazioni del secondo tipo riguardano i contenuti di perizie, di note di qualifica di personale di dipendente, pareri medici, ecc.[35]; come si vedrà *infra*, tale distinguo spiega le sue ricadute pratiche in relazione alla tematica ella rettifica.

Anche i **dati pseudonimizzati** ricadono nella disciplina del Regolamento. Secondo l'art. 4.5, l'attività di pseudonimizzazione consiste nel trattamento dei dati personali in modo tale che gli stessi «*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*». Si tratta di una tecnica cd. ***privacy enhancing***, grazie alla quale il trattamento avviene in modo che le informazioni che consentono ai dati di essere attribuiti ad una persona identificata siano conservate separatamente rispetto al dato pseudonimizzato generato e siano soggette a misure tecniche e organizzative che assicurano tale non – attribuzione[36].

Ponendosi in linea di continuità con le pregresse fonti, il Regolamento fa discendere dalla diversa natura del dato personale la necessità di un grado maggiore o minore di tutela nel compiere le operazioni di trattamento[37].

---

[34] Così E. PELINO, *op.cit.*, 65 il quale richiama le decisioni del Garante del 3 febbraio 2012 (1065256) e del 23 giugno 1998 (39949)

[35] Così E. PELINO, *op.cit.*, 66.

[36] Così L. BOLOGNINI, in BISTOLFI, BOLOGNINI, PELINO, *Il Regolamento privacy europeo, Commentario alla nuova disciplina sulla protezione dei dati personali*, cit., 81. La pseudonimizzazione rientra tra quelle misure tecniche e organizzative funzionali a rendere il trattamento conforme ai requisiti del Regolamento e a tutelare i diritti dell'interessato. È annoverata dall'art. 40.2 tra gli elementi, utilizzati dal titolare o responsabile del trattamento al fine di applicare le disposizioni del Regolamento, enunciabili all'interno dei codici di condotta redatti dalle associazioni e dagli altri organismi rappresentanti le categorie di titolari di trattamento o di responsabili di trattamento. L'applicazione della pseudonimizzazione consente al titolare del trattamento di effettuare un trattamento legittimo, riducendo le minacce alla sicurezza dei dati degli interessati, come evidenziato dall'art. 32.1. Ciò, tuttavia, non pregiudica l'adozione di ulteriori misure di protezione dei dati. La *ratio* stessa della pseudonimizzazione apre alla necessità di una serie di misure funzionali alla riduzione di rischi di reidentificazione non autorizzata, misure che non riguardano solo la protezione da attacchi esterni ma anche i profili di autorizzazione del personale incaricato del trattamento e le cautele messe in atto per tenere al sicuro la chiave segreta utilizzata per la crittografia. Il fatto che le suddette chiavi siano disgiunte dai dati pseudonimizzati, peraltro, non garantisce la loro irreperibilità, per questa ragione è bene adottare misure di sicurezza volte a proteggere l'accesso indebito ai luoghi in cui esse vengono conservate, Quest'aspetto si correla con quello relativo ai profili di autorizzazione, in quanto sarà necessario stabilire chi e con quale modalità potrà avere accesso alle chiavi funzionali ea consentire la reidentificazione.

[37] Cfr. F. DI RESTA, *op.cit.*, 15.

Speciale presidio è apprestato alle informazioni «*che, per loro natura, sono particolarmente 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*» (in tali termini cfr. il *Considerando* n. 51). L'individuazione di categorie particolari di dati personali, pertanto, è funzionale alla previsione di una disciplina più restrittiva per il trattamento[38]. Peraltro, in ragione della maggiore pericolosità del trattamento dei dati genetici, biometrici e dei dati relativi alla salute, il Regolamento autorizza gli Stati membri a mantenere o introdurre ulteriori condizioni ed eventualmente limitazioni alla relativa disciplina.

In dettaglio, l'art. 9 del Regolamento disciplina il trattamento di "*particolari categorie di dati*", ponendosi in continuità con le pregresse fonti relative ai **dati sensibili**, ma arricchendo tuttavia il contenuto della categoria: infatti, accanto ai dati relativi alla vita sessuale, aggiunge quelli relativi all'orientamento sessuale nonché i dati genetici e quelli biometrici. In dettaglio, la predetta norma annovera tra i **dati particolari** quelli che non solo identificano l'individuo ma concorrono indefettibilmente alla costruzione della sua identità fisica e sociale[39]. Si tratta dei "*dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, oltre a quelli relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*" (art. 9, primo comma).

Quanto all'**origine razziale**, l'espressione è indicata solo al fine di tutelare la persona oggetto di siffatta catalogazione, ma non implica, come chiarito anche dal *Considerando* n. 51, nessuna adesione da parte del legislatore a teorie che tentano di dimostrare l'esistenza di razze umane distinte.

Quanto ai **dati biometrici**, essi cambiano in maniera irreversibile la relazione tra corpo e identità in quanto le caratteristiche del corpo umano possono essere lette da una macchina e sottoposte a un successivo trattamento[40]. Secondo la definizione di cui all'art. 4, n. 14, del Regolamento, essi sono rappresentati da «*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*». Parte della dottrina[41] evidenzia che connotati di tale categoria ineriscono:

---

[38] Così M. GRANIERI, *op.cit.*, § 2, secondo cui leggendo l'*incipit* dell'art. 9, soprattutto in raffronto all'art. 6, sembrerebbe potersi dire che vi è stato un passaggio da un trattamento condizionato (per tutti i dati) a un divieto di trattamento per quelli rientranti tra le categorie particolari. Soltanto il prosieguo nella lettura dell'art. 9 introduce deroghe alla regola generale, sulla base di una elencazione - par. 2, lett. da *a* a *j* - di circostanze in cui il primo paragrafo non si applica e, dunque, il divieto di trattamento è rimosso.

[39] Così M. GRANIERI, *op.cit.*, § 2.

[40] Così era stato osservato dal gruppo di lavoro *ex* art. 29 (WP29). Cfr. S.RODOTÀ, *op.cit.*, che così scriveva sulla biometria: «l'irrrompere della biometria propone nuovi intrecci tra corpo fisico e corpo elettronico. Il corpo fisico sta diventando una password. Il corpo elettronico, l'insieme dei nostri dati, è oggetto di *un data mining* sempre più aggressivo e capillare, motivato con esigenze di sicurezza o di mercato. La sorveglianza sociale si affida a guinzagli elettronici sempre più sofisticati. Il corpo umano viene assimilato ad un qualsiasi oggetto in movimento, controllabile a distanza con una tecnologia satellitare o utilizzando le radiofrequenze. Davanti a noi sono mutamenti che toccano l'antropologia stessa delle persone. Siamo di fronte a slittamenti progressivi: dalla persona "scrutata" attraverso la videosorveglianza e le tecniche biometriche si può passare ad una persona "modificata" da diversi strumenti elettronici, dall'inserimento di *chip* ed etichette "intelligenti", in un contesto che sempre più nettamente ci trasforma in "*networked persons*", persone perennemente in rete, via via configurate in modo da emettere e ricevere impulsi che consentono di rintracciare e ricostruire movimenti, abitudini, contatti, modificando così senso e contenuti dell'autonomia delle persone, e quindi incidendo sulla loro dignità».

[41]Così E. PELINO, *op.cit.*, 70 s. Sulla nozione di dato biometrico cfr. I.A. CAGGIANO, *Pagamenti non autorizzati tra responsabilità e restituzioni. una rilettura del d. legisl. 11/2010 e lo scenario delle nuove tecnologie*, in *Riv. dir. civ.*, 2016, 2, 459 ss., secondo cui le tecnologie biometriche permettono di riconoscere in maniera sufficientemente certa e

- ✓ alla tipologia di utilizzo, in quanto sono impiegati di regola come identificativi esclusivi;
- ✓ alla funzione di identificazione e di autenticazione;
- ✓ alla fonte, poiché sono estrapolati da caratteristiche fisiche, fisiologiche o comportamentali di una persona;
- ✓ all'oggetto, nel senso che recano informazioni uniche sulla persona da cui sono estratte, ottenute con particolari tecniche di misurazione e di analisi matematica.

Senza alcuna pretesa di esaustività, a titolo meramente esemplificativo, costituiscono dati biometrici, tra l'altro le informazioni matematiche elaborate a partire dal volto di una persona, dalle impronte digitali, dalle caratteristiche dell'iride, più in generale da conformazioni di reticoli di capillari, da elementi misurabili dal modo di camminare o di gesticolare. Si annovera, da ultimo, in tale categoria anche la firma grafometrica[42].

Quanto **ai dati relativi alla salute**, detti anche dati sanitari, «*dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio; un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli*

---

immediata un soggetto attraverso i parametri fisici, che, anche quando variabili nel tempo, sono univocamente riconducibili a un'unica persona, non possono essere persi o più agilmente intercettati, come le password, o in ogni caso utilizzati da terzi, né facilmente contraffatti. In altri termini, sono in grado di garantire una ragionevole univocità tra utilizzatore titolare e strumento di pagamento. Le tecniche d'identificazione biometrica più diffuse consistono nella lettura e verifica automatizzata di alcuni elementi che, essendo connaturati all'individuo, corrispondono a una sua caratteristica fisica o comportamentale, come le impronte digitali, la geometria della mano, la struttura dell'iride o la conformazione della retina, i tratti del volto, la conformazione scheletrica, la voce o la dinamica di apposizione della firma (c.d. firma grafometrica), l'analisi della struttura del DNA. L'Autrice puntualizza altresì che la verifica del dato biometrico riesce ad assicurare un collegamento affidabile tra l'utilizzatore dello strumento o del servizio e il titolare o legittimo destinatario, sia quando l'identificazione avvenga tramite il raffronto con dati registrati o memorizzati (con costituzione di relativa banca dati, c.d. sistema di identificazione biometrica), sia quando il confronto avvenga con il dato memorizzato all'interno di un supporto durevole nella disponibilità del titolare (c.d. sistema di verifica biometrica).

[42] Per la riconducibilità di tale tipologia di firma all'identificazione biometrica cfr. C. LICINI, *Il notaio dell'era digitale: riflessioni gius-economiche*, in *Notariato*, 2018, 145, il quale così spiega il funzionamento della stessa: «questa tipologia di firma funziona esattamente come avviene su un foglio di carta; nel momento in cui l'utente applica la firma sulla tavoletta biometrica, quel rilevamento dinamico del movimento dello scrivere, la macchina non può riconoscerlo se non quando è fatto dallo stesso essere vivente dello specimen, che quindi deve essere necessariamente …lì, vivo e presente!». Sul tema *adde* I.A. CAGGIANO, *op.cit.*, 459 ss., secondo cui: «un sistema basato sul riconoscimento biometrico, quando svolge la funzione di firma, è, così, in grado di ristabilire una ragionevole certezza giuridica relativamente all'autore del documento e del correlato atto giuridico. Ciò può ridurre, - *de jure condendo* - la necessità, o - *de jure condito* - quanto meno la frequenza, del ricorso, a regole speciali di allocazione del rischio. In altri termini, la connessione univoca tra soggetto e atto nel metodo di autenticazione biometrico, il quale esemplarmente nella firma grafometrica replica - accentuando la certezza circa l'autorialità - la sottoscrizione " analogica ", riconduce l'ambito delle contestazioni relative all'autorizzazione su un terreno vicino, e con margini di certezza superiori, al disconoscimento della sottoscrizione, in ogni caso sganciato dalla libera valutazione del giudicante e da questioni relative ad improbabili memorizzazioni di codici di accesso».

Infine si ricorda, ancora con riferimento alla firma grafometrica, che il Garante, a fronte della complessità della materia in rapporto alla disciplina sul trattamento dei dati personali, ha adottato, con il "Provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014", delle "L*inee-guida in materia di riconoscimento biometrico e firma grafometrica*" onde fornire un quadro di riferimento unitario sulla cui base i titolari possano orientare le proprie scelte tecnologiche, conformare i trattamenti ai principi di legittimità stabiliti dal Codice e rispettare elevati standard di sicurezza.

Il regolamento dedica una previsione *ad hoc alle* fotografie, specificando, al considerando n. 51, che il trattamento *delle stesse* «*non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica*».

effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro» (così *Considerando* n. 35).

Per **dati genetici,** secondo il *Considerando* n. 34, «*è opportuno che si intendano i dati personali relativi alle caratteristiche genetiche, ereditarie o acquisite, di una persona fisica, che risultino dall'analisi di un campione biologico della persona fisica in questione, in particolare dall'analisi dei cromosomi, dell'acido desossiribonucleico (DNA) o dell'acido ribonucleico (RNA), ovvero dall'analisi di un altro elemento che consenta di ottenere informazioni equivalenti*».

Tali dati consistono dunque in una specificazione dei dati sanitari le cui caratteristiche attengono alla fonte, in quanto sono estratti da campioni biologici della persona; all'oggetto, in quanto recano caratteristiche genetiche, ereditarie, o acquisite.

Si osservi, infine, che i dati sensibili potrebbero essere desunti anche da informazioni di per sé non sensibili; si discorre al riguardo di **dati sensibili per inferenza** (abduzione logica)[43].

Il GDPR non fornisce una definizione di **dato giudiziario** ma, come si vedrà *infra*, stabilisce (all'art. 10) disposizioni specifiche per il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

4. Il trattamento dei dati personali: principi, condizioni di liceità e sanzioni previste.

Il trattamento dei dati personali è l'attività, di qualsiasi genere, svolta su dati personali[44] e, secondo il Considerando n. 4, «*dovrebbe essere al servizio dell'uomo*»[45].

Secondo il Regolamento (vd art. 4, n.2), esso consiste in «*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*

[43] Così E. PELINO, *op.cit.*, 72, il quale riporta l'esempio della scelta di un passeggero di prenotare un particolare menù in volo, diverso dal menù *standard*, posto che siffatta preferenza può indicare l'appartenenza religiosa o filosofica oppure intolleranze alimentari.

[44] Così E. PELINO, *op.cit.*, 86.

[45] Su quest'espressione del Regolamento cfr., criticamente, G. ALPA, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contratto e impr.*, 2017, 3, 723, il quale, dopo una concisa quanto efficace riflessione in merito al concetto di identità personale, e alla relativa evoluzione nel corso del tempo, obietta che: «potrebbe addirittura apparire ipocrita l'assunto contenuto nel considerando n. 4 del Regolamento europeo (…). In realtà, proprio la funzione del Regolamento consiste nel rafforzare i presidi della persona e dei suoi dati rispetto ad un mercato (non solo europeo, ma globalizzato) che ne postula la libera circolazione e appropriazione al fine di poterne sfruttare l'utilità commerciale. Ed infatti il Regolamento introduce nuovi diritti a favore dell'interessato con riguardo ai dati trasmessi al di fuori dell'Unione, il diritto alla revoca del consenso del trattamento a fini di *marketing* diretto, e speciali garanzie a tutela dei minori. Fissa inoltre regole più stringenti in materia di responsabilità e di solidarietà tra i soggetti titolari dei dati e rafforza la tutela dei dati assoggettati alla circolazione al di fuori dell'Unione. Non è quindi accettabile l'idea che la persona eserciti un diritto di proprietà sui propri dati e ne possa disporre liberamente: la dimensione digitale è un prolungamento della dimensione umana, e come alla persona non si consente di alienare parti del corpo che potrebbero comprometterne la funzionalità, allo stesso modo si dovrebbe proibire la cessione volontaria di dati personali che sono particolarmente "sensibili". I diritti fondamentali sono indisponibili, sì che la cessione di dati che potrebbero essere utilizzati per procurare danno alla persona non dovrebbe essere consentita, neppure se vi fosse il consenso dell'interessato».

l'interconnessione, la limitazione, la cancellazione o la distruzione». È definita (dal successivo punto 4 dell'art. 4) **attività di 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*».

Il legislatore europeo ha individuato una serie di basi giuridiche dalle quali dipende la liceità del trattamento (artt. 6 e 9 reg. 2016/679) ed ha finanche sancito una serie di canoni e criteri ai quali quest'ultimo va improntato, pena, nonostante la sussistenza di una base giuridica, l'illiceità del trattamento (art. 5 reg. 2016/679): canoni e criteri che, alla luce della loro indeterminatezza e soprattutto del loro carattere di direttive fondamentali della disciplina, vengono designati come **principi del trattamento**[46].

Quanto alle **modalità di trattamento**, il Regolamento impone obblighi di informazione, di comunicazione (artt. 12-15 reg. 2016/679), di registrazione dell'attività di trattamento (art. 30 reg. 2016/679), di adozione di misure tecniche e organizzative di sicurezza (art. 32 reg. 2016/679)[47], nonché di notifica all'Autorità di controllo e di comunicazione all'interessato delle eventuali violazioni dei dati personali (artt. 33 e 34 reg. 2016/679), di valutazione d'impatto sulla protezione dei dati (art. 35 reg. 2016/679), etc.

Parte della dottrina[48] evidenzia che s'instaura **tra interessato e titolare un rapporto giuridico** di cui gli **obblighi informativi** devono precisare i seguenti tratti determinativi: a) l'identità e il contatto del titolare e del suo rappresentante; b) l'identità e il contatto del responsabile; c) la base giuridica e la finalità del trattamento; d) gli eventuali destinatari o le categorie di destinatari dei dati; e) l'eventuale intenzione del titolare di trasferire i dati personali a un paese terzo o a un'organizzazione internazionale; infine, nella fattispecie dell'acquisizione dei dati non dall'interessato, anche f) le categorie di dati ottenuti.

Quanto ai **principi** che devono governare questo rapporto, il Regolamento si pone in linea di continuità con la direttiva 95/46 e (all'art. 5) raccoglie, pur presentando diversi arricchimenti e specificazioni, la lunga tradizione internazionalistica in materia di *privacy*, fondata su trattati universali, come la Dichiarazione universale dei diritti umani adottata dalle Nazioni Unite nel 1948

---

[46] F. PIRAINO, *op.cit.*, 386.

[47] «L'art. 32 del Regolamento impone, infatti, che il titolare e il responsabile del trattamento debbano attuare tutte le misure tecniche ed organizzative utili a garantire un livello di sicurezza adeguato al rischio. L'obbligo tecnico-organizzativo è modulato tenendo in considerazione quattro distinti fattori: i) lo stato dell'arte; ii) i costi di attuazione; iii) la natura, l'oggetto, il contesto e le finalità del trattamento; iv) il rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche. Proprio con riferimento all'ultimo fattore, il secondo comma dell'art. 32 sottolinea che la valutazione dei rischi sottesi all'adeguatezza del livello di sicurezza debba essere attuata tenendo in particolare considerazione la possibilità che il trattamento possa ingenerare fattispecie lesive quali la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso – in modo accidentale o illegale – ai dati personali trasmessi, conservati o comunque trattati. (…). Il primo comma dell'articolo in commento enuncia poi, in via meramente preventiva l'anonimato parziale all'interessato e, comunque, uno status sufficiente a proteggere gli elementi di un determinato dato tali da identificare o rendere identificabile una persona fisica. (….). Secondo il quarto ed ultimo comma dell'art. 32, è onere del titolare e del responsabile quello di formare e rendere edotto, in merito alle politiche di sicurezza del trattamento adottate, ogni soggetto che ha accesso ai dati personali è chiamato ad operare sotto la propria autorità. (…). Nel quadro prescrittivo sin qui delineato si installa il terzo comma dell'art. 32, che incentiva l'adozione di codici di condotta e/o di meccanismi di certificazione (di cui agli artt. 40 e 42 reg. cit.), indicandone la rilevanza e l'utilità quali elementi probatori idonei a confermare la conformità delle misure tecnico-organizzative prescelte rispetto alle prescrizioni normative» S. VIGLIAR, Data breach *e sicurezza informatica*, in *La nuova disciplina europea della* privacy, a cura di S. SICA-V. D'ANTONIO-G.M. RICCIO, Padova, 2016, 248 ss. Con riferimento a questo ultimo aspetto in particolare, cfr. Considerando 77 del Regolamento.

[48] Così F. PIRAINO, *op.cit.*, 390 s..

e il Patto per i diritti umani e politici del 1966, e su trattati regionali, come la Convenzione europea dei diritti dell'uomo del 1950[49].

Tali principi consistono:

a) nella liceità, correttezza e trasparenza;
b) nella limitazione della finalità del trattamento: il trattamento dei dati personali presuppone una finalità[50] **determinata, esplicita, legittima e modalità di utilizzo compatibili** con tale finalità[51];
c) nella minimizzazione dei dati, che si traduce nell'acquisizione di dati adeguati, pertinenti e limitati a quanto strettamente necessario alla finalità del trattamento[52];
d) nell'esattezza, che include anche l'eventuale aggiornamento dei dati e l'adozione di misure ragionevoli per cancellarli o rettificarli ove inesatti rispetto alla finalità per cui sono trattati[53];
e) nella limitazione della conservazione dei dati in forma identificativa dell'interessato solo per l'arco temporale necessario al conseguimento della finalità del trattamento[54];
f) nell'integrità e riservatezza, intese come l'obiettivo della sicurezza dei dati perseguito tramite l'adozione di misure tecniche e organizzative in grado di prevenire i trattamenti non autorizzati o illeciti, la perdita o la distruzione dei dati, i danni accidentali[55];

[49] Cfr. F. PIRAINO, *op.cit.*, 390 s..

[50] Il principio di finalità è enunciato dall'art. 5, lett. b, secondo il quale i dati sono «raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali ("limitazione della finalità")». Per la prassi dei precedenti del Garante, cfr. Garante Privacy, 10 giugno 2003, doc web n. 29836.

[51] Sul principio di finalità del trattamento, cfr. F. DI RESTA, *op. cit*., 44 ss. in particolare con riferimento alla trattazione della questione della trasformazione delle finalità del trattamento, come nel caso in cui una lista di nominativi raccolti durante una campagna referendaria sia poi ceduta ad un'organizzazione per effettuare *marketing* diritto. Altra ipotesi ivi richiamata è quella oggetto di una nota pronuncia di legittimità (Cass., 8 luglio 2005, n. 14390, in *Corr. giur*., 2006, 1, 39, con nota F.M. CIRILLO, *Il trattamento dei dati sensibili e l'utilizzazione in ambito giudiziario del materiale probatorio raccolto dagli investigatori privati*), che, in linea con un suo precedente, ha ribadito come le norme sulle *privacy* «hanno ad oggetto della tutela anche i dati già pubblici o pubblicati, poichè colui che compie operazioni di trattamento di tali informazioni, dal loro accostamento, comparazione, esame, analisi, congiunzione, rapporto od incrocio, può ricavare ulteriori informazioni e, quindi, un "valore aggiunto informativo", non estraibile dai dati isolatamente considerati, potenzialmente lesivo della dignità dell'interessato (ai sensi degli artt. 3, primo comma, prima parte, e 2 della Costituzione), valore sommo a cui è ispirata la legislazione sul trattamento dei dati personali" (Corte di Cassazione, sez. 1, sent. n. 11864 del 2004)».

[52] Il principio di minimizzazione dei dati è stabilito dall'art. 5, lett. c, secondo il quale i dati sono «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati")». Per la prassi dei precedenti del Garante, cfr. Garante Privacy, 8 marzo 2007, doc. web n. 1391803.

[53] Il principio di esattezza è prescritto nell'art. 5, lett. d, secondo il quale i dati sono «esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza")». Per la prassi dei precedenti del Garante, Garante Privacy, 7 dicembre 2016, doc. web n. 5947202.

[54] Il principio di conservazione è prescritto nell'art. 5, lett. e, secondo il quale i dati sono «conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato ("limitazione della conservazione")». Per la prassi dei precedenti del Garante, Garante Privacy, 27 dicembre 2001, doc. web n. 39696.

[55] Il principio di integrità e riservatezza è prescritto nell'art. 5, lett. f, secondo il quale i dati sono «trattati in maniera da garantire un'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 ("integrità e riservatezza")».

g) nella responsabilizzazione del titolare, intesa come onere di comprovare il rispetto di tutti i requisiti summenzionati.

Il trattamento dei dati personali è lecito se effettuato in presenza di **specifiche basi giuridiche**, indicate dall'art. 6 in modo non difforme dal nostro cod. *privacy* (art. 24) e relative:

a) al consenso;
b) **all'adempimento di obblighi contrattuali;**
c) agli interessi vitali della persona interessata o di terzi;
d) **all'obbligo legale cui è soggetto il titolare;**
e) **all'interesse pubblico o esercizio di pubblici poteri**;
f) all'interesse legittimo o prevalente del titolare o di terzi cui i dati vengono comunicati[56].

Fra questi requisiti di trattamento, meritano una particolare attenzione per i profili di interesse notarile:

- l'adempimento degli obblighi contrattuali;

- l'adempimento un obbligo legale al quale è soggetto il titolare del trattamento;

- l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

- il consenso dell'interessato.

[56] In base al *Considerando* 47: «I legittimi interessi di un titolare del trattamento, compresi quelli di un titolare del trattamento a cui i dati personali possono essere comunicati, o di terzi possono costituire una base giuridica del trattamento, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento».

Sempre in base al medesimo Considerando, l'interesse legittimo è riscontrabile ad esempio quando «esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, ad esempio quando l'interessato è un cliente o è 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 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».

Nel successivo *Considerando* 49 si meglio precisa che «Costituisce legittimo interesse del titolare del trattamento interessato 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».

La principale peculiarità della disciplina fin qui descritta risiede nel fatto il bilanciamento fra interesse legittimo del titolare, da un lato, e interessi o i diritti e le libertà fondamentali dell'interessato, dall'altro, non compete più alla Autorità ma costituisce un onere del titolare, fermo restando che le Autorità potranno sempre verificare la correttezza del suo adempimento.

La prima base giuridica che informa l'attività del Notaio è rappresentata dall'**adempimento di obblighi contrattuali**: basti al riguardo ricordare che il Notaio è obbligato a prestare il suo ministero ogni volta che ne è richiesto (così recita l'art. 27 legge not.).

Quanto all'**esecuzione di un compito di interesse pubblico** o all'**adempimento di un obbligo legale**[57], si pensi all'obbligatorietà del trattamento e della conservazione dei dati personali cui il Notaio deve attendere in ossequio alle prescrizioni della legge notarile, sia in riferimento agli originali degli atti sia in ordine ai repertori e agli indici delle parti; si pensi ancora agli adempimenti che la normativa civilistica attribuisce al Notaio, ad esempio con riguardo alla cura che la trascrizione venga eseguita nel più breve tempo possibile, pena il risarcimento del danno in caso di ritardo[58]. Infine, si ricordi che la disciplina di carattere tributario e di antiriciclaggio impone al Notaio ulteriori compiti che ineluttabilmente richiedono trattamento di dati personali.

Positivizzato nell'art. 6, paragrafo 1, lett. C, il trattamento dei dati personali per l'adempimento di un obbligo legale è assoggettato alla disciplina giuridica comunitaria oppure nazionale, a seconda che l'obbligo legale vada individuato con riferimento:

a) all'ordinamento dell'Unione Europea;

b) oppure al diritto dello Stato membro cui è soggetto il titolare del trattamento.

Stando infatti alla previsione dell'art. 6, paragrafo 3, ed ai *Considerando* 10[59] e 45[60] del Regolamento, gli Stati membri rimangono liberi di mantenere oppure di introdurre norme nazionali

---

[57] «Va, innanzitutto, evidenziato che ciascuna delle sei condizioni di liceità dettate dal Regolamento è da sola sufficiente a legittimare il trattamento; tutte si pongono su di un piano di assoluta parità e importanza. L'esistenza di una sola di esse fa venir meno il divieto generale avente ad oggetto il trattamento, dei dati, senza necessità di indagare sulle altre» M. RAFFAGHELLI, *I principi applicabili*, in *Adempimenti privacy per professionisti e aziende*, C. CORRADO-F. D'AMORA e F. FIORE (a cura di), Milano, 2018, 45.

[58] In dottrina cfr. E. LUCCHINI GUASTALLA, *op.cit.*, 111.

[59] *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. È opportuno assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione. Per quanto riguarda il trattamento dei dati personali per l'adempimento di un obbligo legale, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del presente regolamento. In combinato disposto con la legislazione generale e orizzontale in materia di protezione dei dati che attua la direttiva 95/46/CE gli Stati membri dispongono di varie leggi settoriali in settori che richiedono disposizioni più specifiche. Il presente regolamento prevede anche un margine di manovra degli Stati membri per precisarne le norme, anche con riguardo al trattamento di categorie particolari di dati personali («dati sensibili»). In tal senso, il presente regolamento non esclude che il diritto degli Stati membri stabilisca le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito».

[60] *Considerando* 45: «È opportuno che il trattamento effettuato in conformità a un obbligo legale al quale il titolare del trattamento è soggetto o necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri sia basato sul diritto dell'Unione o di uno Stato membro. Il presente regolamento non impone che vi sia un atto legislativo specifico per ogni singolo trattamento. Un atto legislativo può essere sufficiente come base per più trattamenti effettuati conformemente a un obbligo legale cui è soggetto il titolare del trattamento o se il trattamento è necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri. Dovrebbe altresì spettare al diritto dell'Unione o degli Stati membri stabilire la finalità del trattamento. Inoltre, tale atto legislativo potrebbe precisare le condizioni generali del presente regolamento che presiedono alla liceità del trattamento dei dati personali, prevedere le specificazioni per stabilire il titolare del trattamento, il tipo di dati personali oggetto del trattamento, gli interessati, i soggetti cui possono essere comunicati i dati personali, le limitazioni della finalità, il periodo di conservazione e altre misure per garantire un trattamento lecito e corretto. Dovrebbe altresì spettare al diritto dell'Unione o degli Stati membri stabilire se il titolare del trattamento che esegue un compito svolto nel pubblico

per meglio specificare la disciplina di trattamento dei dati personali per l'adempimento di un obbligo legale.

Quanto al **consenso dell'interessato**, il Regolamento si preoccupa di offrirne una definizione (all'art. 4, n. 11) affermando che esso consiste in qualsiasi manifestazione di volontà 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 siano oggetto di trattamento[61]. Il consenso deve pertanto sostanziarsi in «una dichiarazione: *libera*, cioè espressa in modo volontario senza coercizione; *specifica*, cioè avente uno scopo preciso; *informata*, nel senso che deve presupporre la valutazione e comprensione dei fatti e delle conseguenze correlate ed infine *esplicita*, cioè prestata attivamente»[62].

Oltre che nell'art. 4, la disciplina del consenso è contenuta anche nell'art. 7, con riferimento sia alla fase preconsensuale sia a quella successiva relativa all'eventuale revoca, nonché nell'art. 8 con riguardo al consenso del minore.

Per un verso, rispetto alla fase preconsensuale, l'art. 7 ha cura di stabilire che il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali. È in questa direzione che si giustifica la lettera del paragrafo 4 dell'articolo in commento nella parte in cui ammette che per valutare se il consenso sia stato liberamente prestato, «*si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto*». Si intende, con tali termini, scongiurare ipotesi di abusi dell'obbligo contrattuale di raccogliere i dati personali dell'interessato, che celino delle vere estorsioni del consenso al trattamento onde perseguire finalità estranee al contratto.

Peraltro, con riferimento alla fase successiva al consenso prestato, l'art. 7 al paragrafo 3 riconosce all'interessato il diritto di revocare il proprio consenso in ogni momento. **La revoca**, atto recettizio e a forma libera, fa venire meno il consenso precedentemente prestato con efficacia *ex*

---

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, quali la sanità pubblica e la protezione sociale e la gestione dei servizi di assistenza sanitaria, di diritto privato, quale un'associazione professionale».

[61] Così E. LUCCHINI GUASTALLA, *op.cit.*, 111. I requisiti di validità del consenso sono desumibili dall'art. 4 nonché dai *Considerando* 42 e 43 mentre le caratteristiche sono maggiormente delineate nell'art. 7 e nel *Considerando* 32: «Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito *web*, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso».

In dottrina diffusamente trattate in S. THOBANI, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Eur. dir. priv*., 2016, p. 513 ss. Quanto alla prova del consenso, si osserva come «Il codice della privacy prevedeva all'art. 23.3. che il consenso dovesse essere documentabile per iscritto. Il requisito non trova espressione nel Regolamento. L'art. 7.1 RGPD pone l'onere della prova del consenso in capo al titolare del trattamento ma la prova potrà essere assolta secondo i criteri generali ammessi dall'ordinamento» (E. PELINO, *Diritti dell'interessato*, in L. BOLOGNINI - E. PELINO - C. BISTOLFI, *Il Regolamento* Privacy *europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, 224).

[62] G. SPOTO, *Disciplina del consenso e tuela del minore*, in *La nuova disciplina europea della privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Padova, 2016, 113.

nunc[63]. È importante notare che la revoca **si pone in stretta relazione con il diritto al consenso,** tanto che non trova applicazione nelle ipotesi in cui non trova applicazione quest'ultimo. Il suo utile effetto finale è quello di caducare il trattamento senza bisogno di ulteriori attività da parte dell'interessato. Venendo meno la base giuridica sulla quale si fonda il trattamento, il titolare ha l'obbligo di cancellare i dati senza ingiustificato motivo, ovviamente, «se non sussiste altro fondamento giuridico per il trattamento» (art. 17, paragrafo 1, lett. b)[64].

Riguardo poi al **consenso del minore**, l'art. 8 stabilisce che:

«1. Qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.

Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni.

2. Il titolare del trattamento si adopera 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.

3. Il paragrafo 1 non pregiudica le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore»[65].

Con questa previsione normativa[66], il legislatore europeo - come rilevato in dottrina - «ha così previsto una sorta di "maggiore età digitale" qualora il consenso al trattamento dei dati, (…), sia espresso da un "grande minore" di 16 anni»[67].

---

[63] Così, E. PELINO, *Diritti dell'interessato,* in L. BOLOGNINI - E. PELINO - C. BISTOLFI, *Il Regolamento* Privacy *europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, 224. Ivi, p. 243, per una distinzione anche concettuale fra revoca del consenso e opposizione al trattamento, avendo entrambi in comune un trattamento per oggetto e determinandone la relativa cessazione.

[64] «Pertanto, la revoca del consenso fa venir meno l'unica base giuridica per quel determinato trattamento di dati: ne deriva che qualsiasi ulteriore trattamenti di dati è illecito. Tuttavia l'art. 7 chiarisce che la revoca del consenso non può avere valore retroattivo: "la revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca ". Beninteso, tale specificazione non vuol dire che si potrà continuare un trattamento iniziato in base ad un valido consenso prestato nel passato. Vuol dire, piuttosto, che la mera revoca del consenso non può comportare la cancellazione stessa dei dati e l'eliminazione di tutti gli effetti del trattamento fino ad allora effettuato» G. MALGIERI, *Diritto di revocare il consenso,* in *Manuale per il trattamento dei dati personali*, G. COMANDÈ e G. MALGIERI, Milano, 2018, 45.

[65] *Considerando* 38: «I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, 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 consenso del titolare della responsabilità genitoriale non dovrebbe essere necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente a un minore».

[66] Per una prima applicazione giurisprudenziale della normativa, cfr., Trib. Mantova, 19 settembre 2017, in *Fam. dir*., 2018, 380: «L'inserimento delle foto dei figli minori sui social network, nonostante l'opposizione di uno dei genitori, integra violazione dell'art. 10 c.c., che vieta la pubblicazione di foto e immagini senza il consenso dell'avente diritto, degli artt. 4, 7, 8 e 145 del D.Lgs. n. 196/2003 (Codice in materia di protezione dei dati personali), riguardante la tutela della riservatezza dei dati personali, degli artt. 1 e 16, comma 1 della Convenzione di New York sui Diritti del

A quanto precede bisogna aggiungere poi - in linea con quanto anticipato *supra* - che il consenso costituisce uno dei presupposti per il **trattamento dei dati** innanzi meglio descritti con riferimento alle regole (dettate dall'art. 9 ed) inerenti ad **alcune particolari categorie di dati personali**.

Rispetto a questi dati, giova segnalare che **il loro trattamento è vietato salvo che**:

a) l'interessato abbia prestato il proprio consenso esplicito per una o più finalità specifiche;

b) il trattamento sia 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;

c) il trattamento sia 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;

d) il trattamento sia 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;

e) il trattamento riguardi dati personali resi manifestamente pubblici dall'interessato;

f) il trattamento sia **necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;**

g) il trattamento sia necessario per motivi di interesse pubblico rilevante;

h) il trattamento sia 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; peraltro, in tal caso, i dati devono essere trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli stati membri o alle norme stabilite dagli organismi nazionali competenti;

i) il trattamento sia necessario per motivi di interesse pubblico nel settore della sanità pubblica;

j) il trattamento sia necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Fra queste ipotesi di deroga, particolarmente interessanti sotto l'angolo di osservazione notarile sembrano essere le disposizioni che consentono il trattamento dei dati personali, fuori dai casi in cui vi è consenso dell'interessato, laddove esso sia necessario per la difesa in giudizio o per motivi di interesse pubblico rilevante, ovvero concerna dati resi manifestamente pubblici dall'interessato: si pensi al riguardo ai dati confluiti in pubblici registri[68].

Fanciullo (Conv. NY 20.11.1989, ratificata dall'Italia con L. 27 maggio 1991, n. 176) e dell'art. 8 del Reg. UE n. 679/2016».

[67] M. NITTI, *La pubblicazione di foto di minori sui social network tra tutela della riservatezza e individuazione dei confini della responsabilità genitoriale*, in *Fam. dir*., 2018, 392. Ivi, si rileva anche come «il recente intervento normativo europeo, da un lato, mostra di dedicare maggiore attenzione ai minori ma, dall'altro, si fa espressione delle loro istanze autonomistiche e personalistiche in considerazione dell'accesso frequente, a volte quotidiano, degli stessi ai servizi della società dell'informazione».

[68] Sebbene risalente, a tale riguardo, giova ricordare, Trib. Roma, 10 febbraio 2003, in *Dir. inform*., 2003: «Il registro dei protesti costituisce ai sensi della l. 12 febbraio 1955 n. 77 un pubblico registro consultabile da chiunque. Pertanto i dati in esso contenuti possono essere trattati ai sensi dell'art. 12 lett. c) e art. 20 lett. b) l. n. 675 del 1996 senza il consenso dell'interessato».

Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

Il **mancato rispetto** delle regole previste, all'interno del GDPR in relazione al **trattamento di particolari categorie di dati**, può comportare le seguenti **sanzioni**:

- sanzioni amministrative pecuniarie sino all'importo di 20.000 000 Euro, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. L'art. 83 del Regolamento detta le condizioni generali per infliggere sanzioni amministrative pecuniarie stabilendo: che ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte siano in ogni singolo caso effettivo, proporzionate e dissuasive; la natura, la gravità e la durata della violazione; il carattere doloso o colposo della violazione; le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati; eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento; il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

- risarcimento del danno in favore dell'interessato (articolo 82 GDPR);

- divieto di trattamento dei dati personali fino a che non sia posto rimedio alla situazione di non conformità (articolo 58, par. 2, lett. f) GDPR).

Per quanto riguarda infine **il trattamento dei dati giudiziali**, fermo quanto riferito innanzi, l'art. 10 del GDPR, nel fare un espresso rinvio all'art. 6, indica le ipotesi di liceità del trattamento e prevede altresì che il trattamento di questi dati può avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

5. Diritti dell'interessato: definizione e catalogazione da parte dei primi commentatori.

L'espressione diritti dell'interessato «designa una serie di prerogative di natura diversa, ora poteri sostantivi ora rimedi di natura specifica, ai quali la disciplina europea affida il compito di consentire all'interessato di seguire, controllare e indirizzare la circolazione delle proprie informazioni di carattere personale»[69]. La definizione di diritti dell'interessato è ampia, anche in considerazione del complesso di diritti riconosciuto alla persona. Ciò nonostante, taluna dottrina ha cercato di perimetrare in due macroaree il complesso dei diritti dell'interessato. Questi ultimi sono stati così distinti in:

- diritti di natura conoscitiva;
- diritti di controllo.

Quanto ai primi sono quelli di: «- ricevere informazione sul trattamento, ossia il diritto all'informativa (artt. 13 e 14); - richiedere/ottenere informazione sul trattamento e sui dati trattati, vale a dire il diritto di accesso (art. 15); - ricevere informazione su gravi anomalie incorse nel trattamento, ossa il diritto alla comunicazione di una violazione dei dati (art. 34). I diritti di "controllo" possono avere ad oggetto o il trattamento o i dati trattati. Hanno ad oggetto il trattamento i diritti di: - autorizzare il trattamento, ossia il diritto al consenso (artt. 6.1.a), 9.2.a); - modificare il trattamento, ossia il diritto di limitazione (art. 18); - far cessare il trattamento, ossia il diritto di revoca del consenso (art. 7.3) e il diritto di opposizione (art. 21). Hanno ad oggetto i dati i

[69] F. PIRAINO, *op.cit.*, 394.

diritti di: - spostare complessi strutturati di dati, ossia il diritto alla portabilità (art. 20); - modificare i dati, ossia diritti di rettifica e di integrazione (art. 16); - eliminare i dati personali, ossia diritto di cancellazione/oblio (art. 17). Va aggiunto al catalogo un diritto di contenuto negativo, il diritto di non subire decisioni unicamente basate su trattamenti automatizzati (art. 22). L'istituto ha una strettissima aderenza con il riconoscimento dell'autodeterminazione, essendo in effetti volto ad evitare ricomposizioni arbitrarie di profili della persona del tutto sottratti al controllo da parte di quest'ultima»[70].

5.1. Diritto all'informativa.

Fra i diritti dell'interessato, rientra innanzitutto il diritto all'informativa[71].

Questo diritto è stato inteso alla stregua di una pretesa «riconosciuta alla persona di comprendere e prevedere l'ambito di circolazione dei propri dati, le finalità, il soggetto o i soggetti decidenti e di procedere su tale base a un consapevole esercizio dei poteri controllo, come, ad esempio, l'espressione o il diniego del consenso il diritto di opposizione»[72]. L'informativa viene ivi distinta in tre diverse tipologie a seconda che le informazioni siano fornite dal titolare all'interessato: in occasione della raccolta diretta dei dati personali presso l'interessato (**art. 13, c.d. informativa diretta**); in occasione di raccolta indiretta, vale a dire da altro titolare di trattamento, come ad esempio in caso di raccolta dei dati da fonte pubblicamente accessibile, (**art. 14, c.d. informativa successiva[73];** in occasione di un mutamento della finalità rispetto a dati già raccolti in uno dei casi precedenti (**art. 13.3 e 14.4, c.d. informativa ulteriore**).

5.2. Diritti di accesso.

[70] E. PELINO, *op.cit.*, 173 s. Quanto alle modalità di esercizio, Considerando 59: «È opportuno prevedere modalità volte ad agevolare l'esercizio, da parte dell'interessato, dei diritti di cui al presente regolamento, compresi i meccanismi per richiedere e, se del caso, ottenere gratuitamente, in particolare l'accesso ai dati, la loro rettifica e cancellazione e per esercitare il diritto di opposizione. Il titolare del trattamento dovrebbe predisporre anche i mezzi per inoltrare le richieste per via elettronica, in particolare qualora i dati personali siano trattati con mezzi elettronici. Il titolare del trattamento dovrebbe essere tenuto a rispondere alle richieste dell'interessato senza ingiustificato ritardo e al più tardi entro un mese e a motivare la sua eventuale intenzione di non accogliere tali richieste».

[71] È noto il dibattito relativo alla controversa natura giuridica del consenso informato, in considerazione della difficile qualificazione del bene giuridico oggetto delle informazioni personali. Qui ci si limita a segnalazione, in linea con attenta dottrina (G. DI RESTA, *ope cit*., 69 ss.), che sul tema si contrappongono almeno due fondamentali orientamenti: da un lato, la qualificazione del consenso informato come negozio (per taluni, unilaterale, per altri, bilaterale di cessione di dati); dall'altro, la qualificazione del consenso informato come mero atto giuridico autorizzatorio. Se nella prima accezione il dato personale è un bene giuridico e il consenso consiste in un atto negoziale di conferimento dei dati personali, nell'altra qualificazione è la legge, non la volontà delle parti, la fonte che consente, al ricorrere dei presupposti indicati, il conferimento dei dati personali. (alla prima delle due ricostruzioni, sembra iscriversi la dottrina innanzi richiamata. Cfr., ivi, 70 s.).

[72] E. PELINO, *op.cit.* 182. Si rinvia ivi per le informazioni oggetto di accesso, per quanto riguarda forma, modalità, termini dell'accesso, nonché sanzioni amministrative per il caso di inadempimento. In questa sede è importante, per ora, sottolineare in particolare che «gli interessati hanno un diritto ad ottenere informazioni *prima* che il trattamento di dati personali abbia inizio e, successivamente, *durante* il trattamento ogni volta che lo richiedano al titolare. Il diritto di ricevere informazioni *prima* che il trattamento abbia inizio è regolato dai suesposti artt. 13 e 14. In realtà non è definito esplicitamente come un "diritto" degli interessati, ma piuttosto come un "obbligo" dei titolari del trattamento *propedeutico* alla legittimità del trattamento stesso. Al contrario, il diritto a ricevere informazioni *durante* il trattamento è regolato dall'art. 15 (diritto d'accesso)» G. COMANDÈ, *Il diritto di ricevere informazioni e il diritto d'accesso*, in *Manuale per il trattamento dei dati personali*, G. COMANDÈ e G. MALGIERI, Milano, 2018, 45.

[73] Resta fermo e ben inteso che il principio dell'informativa successiva va temperato con il principio contenuto nel considerando n. 62 dispone che: «Per contro, non è necessario imporre l'obbligo di fornire l'informazione se l'interessato dispone già dell'informazione, se la registrazione o la comunicazione dei dati personali sono previste per legge».

Fra le facoltà rientranti nell'ambito dei diritti conoscitivi, vi è il diritto di accesso. Questo diritto viene attuato ad iniziativa dell'interessato il quale ha diritto di conoscere le informazioni di cui all'art. 15[74]. In virtù del riconoscimento di questo diritto «i soggetti hanno una serie di dritti: 1. Ottenere dal titolare del trattamento *la conferma* che sia o meno in corso un trattamento di dati personali che lo riguardano; 2. In tal caso, ottenere l'accesso ai dati personali e dunque *una copia degli stessi*, gratuitamente (per ulteriori copie invece è addebitale un ragionevole costo amministrativo); 3. ottenere una serie di *informazioni relative al trattamento* (simili alle informazioni di cui agli artt. 13 e 14)»[75].

5.3. Diritto di conferma del trattamento.

Il diritto alla conferma del trattamento «consente all'interessato di ottenere dal titolare la conferma dello svolgimento o meno di un trattamento dei propri dati personali e di accedere a questi ultimi mediante rilascio, senza spese, di una copia. Tale diritto si estende anche all'ottenimento di una serie di informazioni relative, in parte, alle caratteristiche dei dati e del trattamento, con particolare riferimento alle garanzie previste dall'art. 46 reg. 2016/679 nel caso che sia ammesso il trasferimento dei dati a un Paese terzo o a un'organizzazione internazionale, e, in parte, ai diritti riconosciuti all'interessato dall'ordinamento»[76].

5.4. Diritto alla comunicazione di una violazione dei dati.

L'art. 34 riconosce il diritto a ricevere la comunicazione in caso di violazione dei dati (su cui vd. *Infra* § in tema di *data breach notification*).

5.5. Diritto alla limitazione del trattamento.

Si annovera tra i diritti dell'interessato anche il diritto alla limitazione del trattamento che più che altro costituisce un mezzo di reazione al trattamento illecito o scorretto. Il riferimento normativo del diritto in esame è contenuto nell'art. 18 in base al quale l'interessato può ricorrere quando: a) egli contesti l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali; b) il trattamento sia illecito e l'interessato si opponga alla cancellazione dei dati personali, preferendo che ne sia limitato l'utilizzo; c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali siano necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; d) l'interessato si sia opposto al trattamento ai sensi dell'articolo 21, par. 1 reg. 2016/679, in attesa

[74] E. PELINO, *op.cit.*, 201. Ivi, per riferimento a forme e modalità per l'istanza e il riscontro e per i termini entro i quali il titolare deve adempiere senza ingiustificato ritardo.

[75] G. COMANDÈ, *Il diritto d'accesso*, in *Manuale per il trattamento dei dati personali*, cit., 48. Sulle modalità di esercizio del diritto di accesso, cfr. *Considerando* 63: «Un interessato dovrebbe avere il diritto di accedere ai dati personali raccolti che la riguardano e di esercitare tale diritto facilmente e a intervalli ragionevoli, per essere consapevole del trattamento e verificarne la liceità. Ciò include il diritto di accedere ai dati relativi alla salute, ad esempio le cartelle mediche contenenti informazioni quali diagnosi, risultati di esami, pareri di medici curanti o eventuali terapie o interventi praticati. Ogni interessato dovrebbe pertanto avere il diritto di conoscere e ottenere comunicazioni in particolare in relazione alla finalità per cui i dati personali sono trattati, ove possibile al periodo in cui i dati personali sono trattati, ai destinatari dei dati personali, alla logica cui risponde qualsiasi trattamento automatizzato dei dati e, almeno quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento. Ove possibile, il titolare del trattamento dovrebbe poter fornire l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali. Tale diritto non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software. Tuttavia, tali considerazioni non dovrebbero condurre a un diniego a fornire all'interessato tutte le informazioni. Se il titolare del trattamento tratta una notevole quantità d'informazioni riguardanti l'interessato, il titolare in questione dovrebbe poter richiedere che l'interessato precisi, prima che siano fornite le informazioni, l'informazione o le attività di trattamento cui la richiesta si riferisce».

[76] F. PIRAINO, *op.cit*., 395.

della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Nel commentare la disposizione contenuta nell'art. 18, taluna dottrina ha osservato che «la limitazione del trattamento consiste nel mutamento ad opera dell'interessato del regime giuridico circolatorio, drasticamente circoscritto alla mera conservazione dei dati oppure a una circolazione assai limitata, giacché possibile solo a seguito dell'esplicito consenso dell'interessato oppure quando esso si riveli necessario all'accertamento, all'esercizio o alla difesa di un diritto in sede giudiziaria o anche alla tutela dei diritti di un'altra persona fisica o giuridica o ancora al perseguimento di un interesse pubblico rilevante dell'Unione o di uno Stato membro. La limitazione è tuttavia revocabile dal titolare, il quale, però, deve darne avviso in anticipo all'interessato. Se le ipotesi di limitazione previste dall'art. 18 reg. 2016/679 a), b) e d) rivestono senza dubbio natura di rimedi, la fattispecie della lett. c) si presenta come una situazione soggettiva sostanziale, che conferisce al titolare il potere di reimpiegare i propri dati personali per esigenze legate alla tutela giurisdizionale dei propri diritti in ossequio all'esigenza di economicità dei mezzi giuridici. In caso di rettifica, di cancellazione e di limitazione del trattamento scatta per il titolare l'obbligo di comunicazione delle operazioni effettuate ai destinatari cui sono stati trasmessi i dati, a meno che ciò non si riveli impossibile o implichi sforzi sproporzionati (art. 19 reg. 2016/679)»[77] .

5.6. Diritto di opporsi.

Il diritto di opposizione rappresenta «una delle espressioni del potere di controllo della persona sui propri dati. È una manifestazione di volontà recettizia che l'effetto, nei casi di legge, di far cessare, in via permanente, un determinato trattamento di dati personali»[78].

La norma di riferimento è costituita dall'art. 21 del Regolamento.

Segnatamente, in continuità con il Considerando 69[79], l'art. 21, paragrafo 1°, reg. 2016/679 sancisce che «L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria».

Allo stesso modo, in linea con il Considerando 70[80], l'art. 21, paragrafo 2 e 3, reg. 2016/679 sanciscono che «Qualora i dati personali siano trattati per finalità di *marketing* diretto, l'interessato

---

[77] F. PIRAINO, *op.cit.*,398 s.

[78] E. PELINO, *I diritti dell'interessato*, in *Il regolamento privacy europeo*, cit., 239. Ivi per approfondimenti relativi ai caratteri, esclusioni e deroghe, esercizio, modalità e termini, nonché per differenze fra diritto di opposizione e revoca del consenso. Quanto poi alla differenza fra opposizione e cancellazione essa risiede nel fatto che, mentre nel primo caso, i dati devono essere eliminati dagli archivi del titolare senza alcun discrimine per la finalità, nel secondo è soltanto inibito un determinato utilizzo dei propri dati.

[79] *Considerando* 69: «Qualora i dati personali possano essere lecitamente trattati, essendo il trattamento necessario per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, ovvero per i legittimi interessi di un titolare del trattamento o di terzi, l'interessato dovrebbe comunque avere il diritto di opporsi al trattamento dei dati personali che riguardano la sua situazione particolare. È opportuno che incomba al titolare del trattamento dimostrare che i suoi interessi legittimi cogenti prevalgono sugli interessi o sui diritti e sulle libertà fondamentali dell'interessato».

[80] *Considerando* 70: «Qualora i dati personali siano trattati per finalità di *marketing* diretto, l'interessato dovrebbe avere il diritto, in qualsiasi momento e gratuitamente, di opporsi a tale trattamento, sia con riguardo a quello iniziale o ulteriore, compresa la profilazione nella misura in cui sia connessa a tale *marketing* diretto. Tale diritto dovrebbe essere

ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto. Qualora l'interessato si opponga al trattamento per finalità di *marketing* diretto, i dati personali non sono più oggetto di trattamento per tali finalità».

Infine, il paragrafo 6, dell'art. 21, reg. 2016/679 stabilisce che «Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico».

Sono queste le tre ipotesi tassative nelle quali l'opposizione può essere esercitata. Se nella prima ipotesi enucleata, l'opposizione può essere rifiutata dal titolare nei due casi ivi indicati, nella seconda ipotesi l'opposizione non può essere rifiutata, mentre nell'ultima l'opposizione può essere rifiutata soltanto nel caso in cui il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.

Gli altri paragrafi dell'articolo in commento disciplinano l'uno l'obbligo di informare l'interessato del diritto di opposizione (cfr. par. 4), l'altro invece le modalità di esercizio del diritto con mezzi automatizzati che utilizzano specifiche tecniche (par. 5).

5.7. Diritto alla portabilità dei dati.

Di particolare interesse è il c.d. diritto alla portabilità dei dati, di cui all'art. 20 e al *Considerando* 68 del Regolamento[81].

In base alla disciplina ivi contenuta l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento[82]. Ha inoltre il diritto di trasmettere tali dati a un altro titolare del

---

esplicitamente portato all'attenzione dell'interessato e presentato chiaramente e separatamente da qualsiasi altra informazione».

[81] F. PIRAINO, *op.cit.*, 381: «La disposizione si rivela assai utile, specie con riferimento alla tutela giurisdizionale dei diritti: basti pensare alle controversie di diritto del lavoro che spesso richiedono l'accesso a informazioni relative al lavoratore e detenute dal datore, per ottenere le quali non di rado è necessario formulare la richiesta di ordini giudiziali di esibizione. La norma ha, tuttavia, una portata ovviamente più ampia e si inserisce, contribuendovi, nel processo di reificazione delle informazioni. Un processo delicato perché la circolazione dei dati personali rappresenta un dato di fatto inconfutabile e di per sé, ovviamente, non pernicioso, ma non implica per necessità logica la traduzione dell'informazione di carattere personale in un bene. Un tale esito comporta, infatti, l'accentuazione della dimensione oggettiva del dato personale rispetto alla dimensione personalistica, giacché il bene giuridico, anche quando immateriale, è per definizione altro dal soggetto: è oggetto, per l'appunto, e, come tale, recide la sua derivazione dalla persona e la sua stessa implicazione in quest'ultima, riducendo i margini per il titolare di influenzarne la circolazione, se del caso inibendola. La china della reificazione delle informazioni di carattere personale presenta, a ben vedere, rischi notevoli».

[82] «In questo senso, il diritto alla portabilità costituisce un'integrazione del diritto di accesso. Un aspetto specifico della portabilità consiste nel suo essere uno strumento con cui gli interessati possono facilmente gestire e riutilizzare dati personali in piena autonomia. I dati in questione devono essere ricevuti "in un formato strutturato, di uso comune e leggibile da dispositivo automatico". Per esempio, un interessato potrebbe voler (…) voler recuperare la rubrica dei contatti di posta elettronica su *web*, magari per costruire una lista degli invitati al proprio matrimonio» Gruppo di Lavoro Articolo 29 per la protezione dei dati, *Linee guida sul diritto alla portabilità dei dati*, Adottate il 13 dicembre 2016, Versione emendata e adottata il 5 aprile 2017, 9, nota 16 (consultabile in *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6058842*).

trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti[83]. L'esercizio di questo diritto non deve ledere i diritti e le libertà altrui[84].

La disciplina appena descritta distingue, quindi, fra una portabilità nella sfera di controllo dell'interessato (in virtù di un diritto alla portabilità c.d. interna) e una portabilità nella sfera di controllo di soggetti terzi rispetto al titolare del trattamento e allo stesso interessato (in virtù di un diritto alla portabilità cd. esterna)[85].

Sono portabili esclusivamente i dati personali che:

- riguardano l'interessato. Il che significa che «un dato anonimo ovvero non concernente l'interessato non ricade nell'ambito di applicazione del diritto in questione. Tuttavia, un dato pseudonimo chiaramente riconducibile all'interessato (per esempio, se l'interessato stesso fornisce il rispettivo elemento di identificazione - v. articolo 11, paragrafo 2) è senza dubbio soggetto all'esercizio del diritto alla portabilità»[86].

- sono stati forniti dall'interessato, dove «alla luce delle finalità sottese al diritto alla portabilità dei dati, l'espressione "forniti dall'interessato" deve essere interpretata in modo estensivo escludendo unicamente "dati inferenziali" e "dati derivati", i quali comprendono i dati personali generati da un fornitore di servizi (per esempio, i risultati prodotti da un algoritmo)»[87].

[83] «L'aspettativa è che (…) il diritto alla portabilità dei dati promuova l'innovazione e la condivisione di dati personali fra titolari del trattamento in piena sicurezza e sotto il controllo dell'interessato. Il diritto alla portabilità può favorire la condivisione controllata e limitata delle informazioni personali fra più soggetti e, quindi, arricchire l'esperienza dell'utente nella fruizione di determinati servizi. La portabilità, inoltre, può favorire la trasmissione e il riutilizzo di dati personali fra più servizi di interesse per il singolo utente» Gruppo di Lavoro Articolo 29 per la protezione dei dati, *Linee guida sul diritto alla portabilità dei dati*, Adottate il 13 dicembre 2016, Versione emendata e adottata il 5 aprile 2017, 9, nota 16 (consultabile in *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6058842*).

[84] «La lesione di cui sopra si configurerebbe, per esempio, se la trasmissione dei dati da un titolare all'altro impedisse a soggetti terzi di esercitare i diritti di cui godono in quanto interessati ai sensi del RGPD – come il diritto di informativa, accesso, ecc. (…). Per esempio, un servizio di posta elettronica via *web* può consentire la creazione di un registro di tutti i contatti (amici, parenti, familiari, ecc.) dell'interessato. Poiché si tratta di dati relativi a e creati da la persona fisica identificabile che desidera esercitare il proprio diritto alla portabilità, il titolare dovrebbe trasmettere all'interessato l'intero contenuto del registro con i messaggi in entrata e in uscita.» Gruppo di Lavoro Articolo 29 per la protezione dei dati, *Linee guida sul diritto alla portabilità dei dati*, Adottate il 13 dicembre 2016, Versione emendata e adottata il 5 aprile 2017, 9, nota 16 (consultabile in *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6058842*).

[85] La distinzione in questi termini si deve a M. RAFFAGHELLI e N. DI IORIO, *I diritti dell'interessato (artt. 12-23)*, in *Adempimenti privacy per professionisti e aziende*, cit., 77 s.. L'Autore rileva come «Il diritto alla portabilità c.d. interna costituisce una integrazione del diritto di accesso e consente agli interessati di gestire e di riutilizzare i propri dati personali. Esso, inoltre, è un utile strumento per poter impedire che i dati vengano persi prima che il titolare provveda alla loro cancellazione. Dall'altro lato, il diritto alla portabilità c.d. esterna potrà costituire uno strumento a supporto della libera circolazione dei dati personali nell'Unione e in favore della libera concorrenza tra i titolari del trattamento (fornitori di servizi), anche tramite il potenziamento della libertà di scelta degli interessati».

[86] Gruppo di Lavoro Articolo 29 per la protezione dei dati, *Linee guida sul diritto alla portabilità dei dati*, Adottate il 13 dicembre 2016, Versione emendata e adottata il 5 aprile 2017, 9, nota 16 (consultabile in *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6058842*).

[87] Gruppo di Lavoro Articolo 29 per la protezione dei dati, *Linee guida sul diritto alla portabilità dei dati*, Adottate il 13 dicembre 2016, Versione emendata e adottata il 5 aprile 2017, 9, nota 16 (consultabile in *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6058842*).

Ultimo aspetto di interesse, oltre ai caratteri differenziali da altri diritti previsti nel Regolamento[88] ed alla disciplina espressa come implicita[89], riguarda l'ambito di applicazione del diritto alla portabilità dei dati.

In base all'art. 20, paragrafo 1, lettera a), del Regolamento, il diritto alla portabilità dei dati:

- si applica ai trattamenti basati:

o sul consenso dell'interessato (nei termini di cui all'articolo 6, paragrafo 1, lettera a), ovvero all'articolo 9, paragrafo 2, lettera a) in caso di dati sensibili);

o su un contratto di cui è parte l'interessato, nei termini di cui all'articolo 6, paragrafo 1, lettera b).

- non si applica:

o «al trattamento 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» (art. 20, paragrafo 3)[90].

5.8. Diritto alla rettifica/integrazione dei dati inesatti.

Altro diritto dell'interessato è il diritto alla rettifica/integrazione dei dati inesatti.

Tale diritto è stabilito dall'art. 16 del Regolamento che costituisce applicazione dei principi di esattezza e di integrità prescritti dall'art. 5, par. 1, lett. d). Esso attribuisce all'interessato il diritto a

[88] Sulla differenza fra diritto alla portabilità dei dati personali e diritto di cancellazione, e fra il primo e il diritto di accesso, G. MALGIERI, *Il diritto alla portabilità dei dati personali*, in *Manuale per il trattamento dei dati personali*, G. COMANDÈ e G. MALGIERI, Milano, 2018, 56. Quanto alla prima differenza «tale specificazione vuole sottolineare che la portabilità dei dati dal titolare A al titolare B non implica anche una cancellazione dai dati presso il titolare A. In altri termini, non si tratta di un diritto alla "portabilità" *tout court* (inteso come "prendi-e-porta via", come era invece previsto inizialmente nelle proposte di regolamento), ma un diritto alla *replicabilità* dei trattamenti». Quanto alla distinzione con il diritto di accesso, va detto che, sebbene entrambi includono il diritto di ricevere una copia di dati, la differenza risiede nel formato, tanto è vero che «se per il diritto d'accesso (art. 15) non è richiesta alcuna specifica caratteristica tecnica per la copia dei dati da fornire all'interessato, per il diritto alla portabilità è richiesto "un formato strutturato, di uso comune e leggibile da dispositivo automatico"» (*ivi*, 56).

[89] Nell'art. 20 del Regolamento sono state poi ravvisate delle norme di bilanciamento: l'una, esplicita, l'altra, implicita. «La norma esplicita è al paragrafo 4: il diritto a ricevere e trasferire copia di dati "non deve ledere i diritti e le libertà altrui". Dunque non devono essere coinvolti dati di terze persone; o informazioni protette dalla proprietà intellettuale. Al tempo stesso tale diritto non deve costituire una barriera all'ingresso nel mercato da parte di un titolare (ad es. causa di eccessivo aggravio economico), trattandosi altrimenti di una violazione del diritto all'impresa e d'iniziativa economica. Una norma di bilanciamento implicita, invece, può scorgersi nell'espressione "se tecnicamente fattibile" riferita al trasferimento diretto di dati da un titolare ad un altro» G. MALGIERI, *Il diritto alla portabilità dei dati personali*, cit., 57.

[90] In altri termini, la portabilità non si applica «qualora il trattamento sia 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, ovvero qualora il titolare agisca nell'esercizio di funzioni pubbliche o per l'adempimento di un obbligo legale. Ne deriva che un titolare non è tenuto a prevedere procedure di portabilità in casi del genere» Gruppo di Lavoro Articolo 29 per la protezione dei dati, *Linee guida sul diritto alla portabilità dei dati*, Adottate il 13 dicembre 2016, Versione emendata e adottata il 5 aprile 2017, 9, nota 16 (consultabile in *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6058842*). Si rinvia ivi per approfondimenti e chiarimenti riguardo alle ulteriori questioni relative all'ambito di applicazione del diritto, al suo bilanciamento con le norme generali che disciplinano l'esercizio dei diritti degli interessati, nonché alle modalità attraverso le quali devono essere messi a disposizione i dati portabili.

ottenere senza ritardo dal titolare la rettifica dei propri dati personali inesatti, nonchè l'integrazione di quelli inesatti, anche attraverso il rilascio di una dichiarazione integrativa[91].

In subiecta materia, si è distinto tra dati oggettivi e dati valutativi. In particolare, si ritiene che «ancorché ciò non sia espressamente indicato, la rettifica può riguardare soltanto dati oggettivi e non anche dati valutativi, come chiariva opportunamente l'art. 8.4. cod. priv., essendo logicamente inapplicabili parametri di inesattezza a posizioni giuridiche altrui». Pertanto, i dati soggettivi, in linea generale, non possono essere rettificati, benché entro certi limiti possono subire delle integrazioni[92]. Soprattutto, il diritto alla rettifica/integrazione in parola deve essere esercitato, analogamente agli altri diritti fin qui descritti, nel rispetto delle prerogative e delle peculiarità invalicabili dell'atto notarile, il quale, una volta concluso, rimane intangibile e cristallizzato, a tutela degli interessi convolti e come mezzo di prova legale[93]. Così, altro è immaginare, in ipotesi di ragionamento, la richiesta di rettifica di un errore relativo a "dati preesistenti alla redazione" dell'atto notarile, in maniera coerente con i presupposti posti a fondamento dello stesso meccanismo operativo dell'art. 59 *bis* della legge notarile[94]. Altro sarebbe richiedere - ipotesi, questa, invece inammissibile - che si proceda a rettificare dati obiettivi e storicamente immodificabili rispetto all'atto.

5.9. Diritto alla cancellazione.

Il diritto alla cancellazione è prescritto dall'art. 17. Questo diritto è espressione del «potere di riappropriarsi delle informazioni di carattere personale non soltanto come strumento di reazione a un trattamento illecito o scorretto (art. 17, par. 1, lett. d) reg. 2016/679) o come rimedio per ottenere l'adempimento dell'obbligo legale di cancellazione imposto al titolare dal diritto dell'Unione europea o dello Stato membro di appartenenza, ma anche come potere sostanziale di autodeterminazione informativa»[95].

---

[91] F. PIRAINO, *op.cit.*, 395. Pertanto, «Intendendosi per rettifica la comune "correzione" dei dati il cui contenuto risulti inesatto, il Legislatore europeo ha voluto sottolineare la necessità che i dati riguardanti l'interessato siano corretti, tanto che la rettifica medesima, se si pone attenzione all'espressione "senza giustificato ritardo", siano aspetti che rendano plausibile qualsiasi tipo di ritardo nello svolgimento dell'attività medesima. Oltre che della rettifica dei dati personali inesatti, la stessa disposizione contempla anche il caso in cui i dati in possesso del titolare siano incompleti e necessitino di integrazione» M. RAFFAGHELLI e N. DI IORIO, *I diritti dell'interessato (artt. 12-23)*, in *Adempimenti privacy per professionisti e aziende*, cit., 72.

[92] Così E. PELINO, *op.cit.*, 256 che in tal senso richiama anche la decisione del Garante del 17 giugno 1999, n. 48067. Per indicazioni su esclusioni e deroghe, forma, modalità e termini, *ivi*, 262 s.

[93] Feconda la bibliografia sull'argomento. Cfr., almeno, i contributi dottrinari raccolti nell'opera collettanea a cura di P. SIRENA, *L'atto pubblico notarile come strumento di tutela nella società dell'informazione*, in *Quaderni della Fondazione del Notariato*, 2013.

[94] M. LEO, *Osservazioni sulla rettifica degli atti "certificata" dal notaio*, Studio n. 618-2010/C, in *Studi e materiali*, 2011, 1, 49 e ss.

[95] F. PIRAINO, *op.cit.*, 396 s. «Il diritto alla cancellazione [e il c.d. diritto all'oblio (…)] dei propri dati personali nel nuovo Regolamento europeo è descritto come un diritto in forma rafforzata, dal momento che quando esso viene esercitato, il titolare del trattamento non deve solo cancellare i dati personali dai propri archivi, ma deve anche provvedere a dare notizia della cancellazione ai destinatari cui i dati erano stati precedentemente comunicati e, quando abbiano resi pubblici i dati dell'interessato (…), sono tenuti ad informare della richiesta di cancellazione altri titolari che stiano trattando i dati personali cancellati (cfr. art. 19)» G. COMANDÈ, *Il diritto all'oblio*, in *Manuale per il trattamento dei dati personali*, cit., 50. Rispetto a questo rafforzamento vengono poi sottolineati due ulteriori aspetti. «Il primo è che non è richiesto al titolare di effettuare comunicazioni o informazioni sproporzionate o impossibili; tuttavia, la proporzione dei tentativi va misurata anche sulle soluzioni tecniche possibili, e dunque richiede, come in altre attività previste dal Regolamento, una visione d'insieme delle proprie attività di trattamento e delle misure tecniche ed organizzative da porre in essere. L'altro aspetto, pur collegato al precedente, è che per procedere ai (misurati) sforzi di contattare altri titolari o destinatari di comunicazione di dati è evidentemente indispensabile avere chiare se ed a chi i dati personali siano stati comunicati o resi pubblici» (ivi, 53).

Il diritto di cancellazione è esercitabile soltanto nelle ipotesi tassative previste dall'art. 17 reg. 2016/679, più nello specifico, se sussiste uno dei motivi seguenti:

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

b) l'interessato revoca 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 oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;

d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono 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 sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

Se questi sono i presupposti, resta fermo ed impregiudicato che anche il diritto di cancellazione deve essere ragionevolmente bilanciato con gli interessi convolti nell'atto notarile, in considerazione della sua duplice accezione di strumento di tutela dei diritti ed elemento di prova. In quanto documento destinato a pubblici archivi per essere conservato inalterato nel tempo nel suo tenore originario, esso contiene dei dati che non potranno essere cancellati, essendo stati riportati in Registri o atti tenuti secondo la Legge Notarile (L. 89/1913 e s.m.i.), ed acquisiti:

- per l'adempimento di un obbligo legale che richieda il trattamento;

- nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

- ai fini di archiviazione nel pubblico interesse;

- per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

5.10. Diritto all'oblio.

Un aspetto del diritto all'identità personale è il diritto all'oblio[96], «espressione del diritto alla *privacy* delle vicende personali diffuse via *web* che non siano più di pubblico interesse»[97].

[96] Così, Trib. Milano, 28 settembre 2016, in *Danno e Resp*., 2017, 3, 369, con nota G. MINA, *La tutela del diritto all'oblio.* Ancora, «Il diritto all'oblio salvaguarda in realtà la proiezione sociale dell'identità personale, l'esigenza del soggetto di essere tutelato dalla divulgazione di informazioni (potenzialmente) lesive in ragione della perdita (stante il lasso di tempo intercorso dall'accadimento del fatto che costituisce l'oggetto) di attualità delle stesse, sicché il relativo trattamento viene a risultare non più giustificato ed anzi suscettibile di ostacolare il soggetto nell'esplicazione e nel godimento della propria personalità» Trib. Milano Sez. I, 7 giugno 2012, in *Massima redazionale*, 2013, in *www.leggid'italiaprofessionale.it*.

In dottrina, sulla natura 'duplice' del diritto all'oblio, V. D'ANTONIO, *Oblio e cancellazione dei dati nel diritto europeo*, in *La nuova disciplina europea della* privacy, a cura di S. SICA-V. D'ANTONIO-G.M. RICCIO, Padova, 2016, 219. L'A. evidenzia come questa figura «ove intesa quale mero diritto alla cancellazione del dato ed alla cessazione del trattamento, si rivela funzionale alla tutela di uno specifico bene giuridico: i dati personali. Al contrario, se declinato in

Questa esigenza, problematizzata in un celebre intervento[98], viene enucleata nei Considerando 65[99] e 66[100], e trova la sua fonte di regolamentazione nell'art. 17 del Regolamento, in base al quale l'interessato ha il diritto di ottenere dal titolare del trattamento, la cancellazione[101] dei dati personali che lo riguardano senza ingiustificato ritardo, mentre il titolare del trattamento ha a sua volta

---

termini di divieto di ripubblicazione, di diritto alla attualizzazione di un'informazione o, ancora, quale diritto alla deindicizzazione, il bene giuridico tutelato diviene in tutte e tre i casi quello dell'identità personale».

Per una rassegna, ragionata e attenta, delle diverse ricostruzioni, F. AGNINO, *Il diritto all'oblio e diritto all'informazione: quali condizioni per il dialogo?*, in *Danno e resp*., 2018, 104. Già, G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Dir. inform*., 2014, 519.

[97] Trib. Roma Sez. I, 3 dicembre 2015, in *Quotidiano Giuridico*, 2015 nota di FALETTI. Cfr., Cass., 24 giugno 2016, n. 13161, in *Foro it*., 2016, I, 2734, con nota F. PARDOLESI, *Diritto all'oblio, cronaca in libertà vigilata e memoria storica a rischio di soppressione*.

Al tempo di *internet*, lo stretto legame tra il diritto all'oblio e la protezione dati personali è stato recente affermato dalla Corte di giustizia Europea del 13 maggio 2014, C-131/12, c.d. Sentenza *Google Spain o Costeja*, la quale si è occupata di una richiesta di blocco e cancellazione di dati personali richiesta ai sensi della direttiva europea 95/46. Con tale sentenza la Corte di Giustizia ha innanzitutto affermato che anche i motori di ricerca svolgono un trattamento di dati personali, in qualità di titolari, e grazie a ciò anche ad essi si applica la normativa per la protezione dei dati personali. Quanto agli interessi sostanziali sottesi alla richiesta del cittadino di "essere dimenticato", anche in questo caso il conflitto tra il diritto all'oblio e il diritto all'informazione viene risolto dalla Corte equilibrando i due diritti: nessun dato viene cancellato o rimosso dai server e, soprattutto, dai risultati delle ricerche, vengono solo oscurati i risultati restituiti in base al nominativo della persona cui è stato riconosciuto il diritto all'oblio, ma non quelli, pertinenti allo stesso argomento, relativi ad altre chiavi di ricerca: ad esempio se Tizio ha commesso una rapina all'Ufficio postale di Venzone (eletto borgo dell'anno 2017), ed a Tizio - per motivi meritevoli- viene riconosciuto il diritto all'oblio, i più comuni motori di ricerca non potranno più riportare nei risultati delle ricerche effettuate a partire dal nome "Tizio" il fatto "rapina all'Ufficio postale di Venzone"; ma la ricerca sul fatto "rapina all'ufficio postale di Venzone" riporterà ovviamente la notizia completa anche con il nome di Tizio. Sostanzialmente viene riconosciuto il diritto a che la deindicizzazione delle informazioni personali relative ad un determinato fatto sia effettuata dal motore di ricerca e non dal gestore del sito *web* ove la notizia è stata pubblicata» G. ARCELLA, *Il diritto all'oblio per i dati personali cede rispetto alle esigenze di pubblicità legale*, in *Notariato*, 2017, 3, 314.

[98] S. RODOTÀ, *Privacy, libertà, dignità, Discorso conclusivo della Conferenza internazionale sulla protezione dei dati, 26a Conferenza Internazionale sulla Privacy e sulla Protezione dei Dati Personali Wroclaw (PL)*, 14, 15, 16 settembre 2004. L'Insigne Giurista così si interrogava: «Quale dignità rimane ad una persona divenuta prigioniera di un passato interamente in mani altrui, di cui deve rassegnarsi ad essere espropriato?».

[99] *Considerando* 65: «Un interessato dovrebbe avere il diritto di ottenere la rettifica dei dati personali che la riguardano e il "diritto all'oblio" se la conservazione di tali dati violi il presente regolamento o il diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento. In particolare, l'interessato dovrebbe avere 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 sono stati raccolti o altrimenti trattati, quando abbia ritirato il proprio consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al presente regolamento. Tale diritto è in particolare rilevante se l'interessato ha prestato il proprio consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento, e vuole successivamente eliminare tale tipo di dati personali, in particolare da *internet*. L'interessato dovrebbe poter esercitare tale diritto indipendentemente dal fatto che non sia più un minore. Tuttavia, dovrebbe essere lecita l'ulteriore conservazione dei dati personali qualora sia 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».

[100] *Considerando* 66: «Per rafforzare il "diritto all'oblio" nell'ambiente *online*, è opportuno che il diritto di cancellazione sia esteso in modo tale da obbligare il titolare del trattamento che ha pubblicato dati personali a informare i titolari del trattamento che trattano tali dati personali di cancellare qualsiasi *link* verso tali dati personali o copia o riproduzione di detti dati personali. Nel fare ciò, è opportuno che il titolare del trattamento adotti misure ragionevoli tenendo conto della tecnologia disponibile e dei mezzi a disposizione del titolare del trattamento, comprese misure tecniche, per informare della richiesta dell'interessato i titolari del trattamento che trattano i dati personali».

[101] «Il Regolamento *Privacy* EU accomuna, in un'unica disposizione, diritto alla cancellazione dei dati e diritto all'oblio, con una scelta di *drafting* normativo singolare ove le due posizioni giuridiche, pur menzionate in maniera distinta in più parti del testo, vengono poi assimilate e trattate come un tutt'uno in sede di definizione del contenuto del diritto e della relativa disciplina» V. D'ANTONIO, *Oblio e cancellazione dei dati nel diritto europeo*, in *La nuova disciplina europea della* privacy, cit., 199.

l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei seguenti motivi.

Si tratta di presupposti ora di carattere oggettivo ora di carattere soggettivo.

I presupposti di ordine oggettivo sono:

- l'esaurimento delle finalità per le quali i dati sono stati raccolti; il trattamento illecito dei dati; l'adempimento di un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; la raccolta dei dati relativa all'offerta diretta di servizi della società dell'informazione prestati in favore di minori (cfr., art. 8, paragrafo 1);

I presupposti di ordine soggettivo sono:

- la revoca il consenso su cui si basa il trattamento, nonché l'opposizione al medesimo trattamento.

Se questi sono i presupposti, ai nostri fini, preme evidenziare che tale diritto non è esercitabile quando sussistono superiori interessi che, specificamente indicati dal Considerando 73[102], hanno assunto forza vincolante nella lettera dell'art. 17 del Regolamento[103]. Fra questi ultimi, la norma ivi contenuta fa rientrare l'ipotesi in cui il trattamento sia necessario per l'adempimento di un obbligo legale. Si pensi, ad esempio, al «notaio, obbligato a dare pubblicità a un suo atto»[104] nei pubblici registri[105]. A seguito della loro inserzione, l'interessato non ha diritto ad ottenere la cancellazione

[102] *Considerando* 73: «Il diritto dell'Unione o degli Stati membri può imporre limitazioni a specifici principi e ai diritti di informazione, accesso, rettifica e cancellazione di dati, al diritto alla portabilità dei dati, al diritto di opporsi, alle decisioni basate sulla profilazione, nonché alla comunicazione di una violazione di dati personali all'interessato e ad alcuni obblighi connessi in capo ai titolari del trattamento, ove ciò sia necessario e proporzionato in una società democratica per la salvaguardia della sicurezza pubblica, ivi comprese la tutela della vita umana, in particolare in risposta a catastrofi di origine naturale o umana, le attività di prevenzione, indagine e perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, o di violazioni della deontologia professionale, per la tutela di altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, tra cui un interesse economico o finanziario rilevante dell'Unione o di uno Stato membro, per la tenuta di registri pubblici per ragioni di interesse pubblico generale, per l'ulteriore trattamento di dati personali archiviati al fine di fornire informazioni specifiche connesse al comportamento politico sotto precedenti regimi statali totalitari o per la tutela dell'interessato o dei diritti e delle libertà altrui, compresi la protezione sociale, la sanità pubblica e gli scopi umanitari. Tali limitazioni dovrebbero essere conformi alla Carta e alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.».

[103] La scelta del legislatore è stata fortemente criticata da alcuni commentatori. Per riferimenti si rinvia alle considerazioni contenute in F. AGNINO, *Il diritto all'oblio e diritto all'informazione: quali condizioni per il dialogo?*, in *Danno e resp*., 2018, 109; nonché F. DI CIOMMO, *Il diritto all'oblio nel regolamento (UE) 2016/679. Ovvero, di un "tratto di penna del legislatore" che non manda al macero alcunché, in Trattamento dei dati personali e Regolamento UE n. 2016/679*, in *Corr. giur*., Speciali Digitali 2018, 16 ss.

[104] L'esempio si deve a E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contr. e impr*., 2018, 120 ss.. Ivi, per una rassegna delle diverse teorie circa il contenuto del diritto all'oblio da un punto di vista teorico. Per quanto riguarda, invece, ad una delle situazioni di peculiare interesse fra quelle che escludono l'operatività del diritto all'oblio, e cioè a quella contemplata nella lett. b), art. 17, par. 3, reg. UE 2016/679 ovvero quando il trattamento risulti necessario per l'adempimento di un obbligo, cfr. R. SENIGAGLIA, *Reg. UE 2016/679 e diritto all'oblio nella comunicazione telematica. Identità, informazione e trasparenza nell'ordine della dignità personale*, in *Le nuove leggi civili commentate*, 2017, 5, p. 1023.

[105] Con riferimento al rapporto fra pubblica fede e diritto all'oblio, in giurisprudenza, cfr. almeno per la giurisprudenza europea, la pronuncia della Corte di Giustizia Unione Europea Sez. II, 9 marzo 2017, n. 398/15, in *Le Società*, 2017, 820, con il commento di M. PAPPALARDO, *L'accesso al registro delle imprese tra garanzia di trasparenza e diritto all'oblio*; in *Foro it*., 2017, IV, 165, con nota di R. PARDOLESI, *Non c'è diritto all'oblio per i dati personali nel registro delle imprese. O forse sì*; *Nuova giur. civ*., 2017, 7-8, 1023, con nota G. CARRARO, *L'iscrizione nel registro delle imprese come lecita ingerenza nel diritto al rispetto della vita privata*; in *Giur. It*., 2017, 7, 1618, con nota di A. MANTELERO, *Registro delle imprese - dati personali - la corte di giustizia su pubblici registri e c.d.* right to

dei dati iscritti in un pubblico registro, in quanto la loro conservazione è prevista dalla legge per la tutela di un pubblico interesse[106] , come la certezza del diritto e la sicurezza giuridica[107].

Dalla disciplina contenuta nei considerando 65-66-73 e nell'art. 17 del Regolamento risulta evidente allora che «la tendenza, anche a livello eurounitario, è nel senso (cfr. art. 17, comma 1, lett. a) di prescrivere la cancellazione se i "dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati": e, tuttavia, non si dà luogo a cancellazione, se la conservazione dei dati personali sia necessaria (accanto alle ipotesi dell'esercizio del diritto alla libertà di espressione ed ai motivi di interesse pubblico nel settore della sanità pubblica o finalità storiche, statistiche e di ricerca scientifica o per la difesa di un diritto in sede giudiziaria) "b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento", o anche "d) a fini di archiviazione nel pubblico interesse (...), nella misura in cui il diritto di cui al par. 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento"» [108]. Questo significa, in definitiva, che «Il diritto degli interessati "all'oblio", ossia di impedire che le informazioni possano continuare a circolare (…) dopo un determinato periodo di tempo, fa dunque sempre salve specifiche esigenze: fra cui quella di rispettare obblighi di legge a tutela di interessi generali e di ordine e sicurezza pubblica» [109].

6. Le figure coinvolte dal trattamento dei dati personali.

Sono diverse le figure coinvolte dalla disciplina prevista dal G.D.P.R.:

- l'interessato dal trattamento;

---

be forgotten; in *Notariato*, 2017, 3, 314, con nota G. ARCELLA, *Il diritto all'oblio per i dati personali cede rispetto alle esigenze di pubblicità legale*. Ivi si evidenzia che «Il principio di diritto espresso dalla Corte europea è particolarmente importante per la salvaguardia della completezza ed esaustività dei pubblici registri: l'aver ribadito che esistono delle esigenze superiori rispetto agli interessi dei singoli, che permangono nonostante il decorso del tempo, significa che la pubblica fede, connessa a prerogative statuali, è riconosciuta come un valore. La sentenza in commento costituisce un argine anche a tutte quelle richieste, rivolte al Garante italiano, finalizzate all'oscuramento di taluni dati nei registri immobiliari solo perché connessi a trascrizioni pregiudizievoli, poi cancellate, tali richieste sono basate sull'errata convinzione dell'illiceità del trattamento dati da parte pubblico registro, una volta che sia stata disposta una cancellazione di una trascrizione o di una iscrizione: la cancellazione "è una forma di pubblicità negativa con la quale si rende pubblica l'irrilevanza sopravvenuta di una precedente formalità che da quel momento deve considerarsi come non esistente", senza però rendere inconoscibile la formalità oggetto di cancellazione che pertanto deve rimanere consultabile».

[106] Cass., 9 agosto 2017, n. 19761, in *Società*, 2018, 3, 279 nota di E.E. BONAVERA, *Pubblicità commerciale nel registro delle imprese e diritto all'oblio*: «In tema di trattamento dei dati personali, ai sensi dell'art. 8 della CEDU nonché degli artt. 7 e 8 della cd. "Carta di Nizza", l'interessato non ha diritto ad ottenere la cancellazione dei dati iscritti in un pubblico registro ed è legittima la loro conservazione quando essa sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale o alla protezione dei diritti e delle libertà altrui».

[107] Ci si limita qui a ricordare, in ripresa della parte motiva della evocata pronuncia di legittimità, che «a ricordare come la pubblicità giuridica, caratteristica del contemporaneo stato di diritto e fondamento di civiltà, risponda all'interesse generale della conoscibilità a chiunque di determinati fatti giuridici, mediante registri, albi, elenchi, pubblicazioni periodiche ufficiali: che, accessibili a chiunque, e tenuti da un ufficio pubblico, producono "sicurezza giuridica", in quanto danno certezza di fatti giuridicamente rilevanti, favorendo i rapporti economici e sociali. È forse necessario evidenziare che la certezza del diritto non è un bene come gli altri, in quanto portato della stessa statualità: la prima come proiezione in termini giuridici della sicurezza fisica garantita dalla seconda» Cass., 9 agosto 2017, n. 19761, cit.

[108] Cass., 9 agosto 2017, n. 19761, cit.

[109] Ancora, Cass., 9 agosto 2017, n. 19761, cit.

- il titolare e il contitolare del trattamento;
- il Responsabile del trattamento;
- il Rappresentante del titolare e del responsabile del trattamento;
- il Responsabile della protezione dati.

6.1. L'interessato dal trattamento.

L'interessato è la persona fisica identificata o identificabile tramite i dati personali oggetto del trattamento, titolare di una serie di diritti, quali: il diritto ad un'adeguata informativa (artt. 12-13-14); il diritto di accesso (art.15); il diritto di rettifica (art. 16); il c.d. diritto all'oblio (art. 17); il diritto di limitazione del trattamento (art. 18); il diritto di notificazione (art. 19); il diritto alla portabilità dei dati (art. 20); il diritto di opposizione (art. 21); il diritto a non subire profilazioni inconsapevoli (art. 22). Novità del Regolamento rispetto ai diritti previsti dal codice della privacy riguardano: il diritto ad essere informato anche in riferimento al periodo di conservazione dei dati personali, il diritto alla portabilità dei dati e il diritto di proporre reclamo all'autorità di controllo (art. 13); il diritto all'oblio, che esisteva già nel Codice *Privacy* (era compreso nell'elenco dell'art. 7), ma non gli era dedicato un articolo specifico, come invece è nel GDPR (art. 17); il diritto alla limitazione che permette all'interessato di pretendere che il trattamento dei propri dati sia limitato a quanto necessario ai fini della conservazione (art. 18).

6.2. Il Titolare e il contitolare del trattamento.

Il titolare del trattamento 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*» (vd. art. 4, n. 7).

Si tratta del soggetto che ha il potere di determinare le finalità ed i metodi di trattamento dei dati personali ed è, pertanto, giuridicamente responsabile dell'ottemperanza degli obblighi previsti dalla normativa, sia nazionale che comunitaria, in materia di protezione dei dati personali. Il titolare è il primo destinatario al quale vanno indirizzate le richieste di tutela degli interessati al trattamento, in caso di violazione dei diritti.

Il Regolamento disciplina, altresì, la figura del **contitolare del trattamento** (vd. art. 26), la quale ricorre quando «*due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento*». È previsto in particolare che i contitolari determinino in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, salvo che - e nella misura in cui - le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo, il cui contenuto essenziale è messo a disposizione dell'interessato, deve riflettere adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati; in ogni caso, l'interessato può esercitare i propri diritti nei confronti di ciascun titolare del trattamento[110].

Principali obblighi del titolare del trattamento riguardano:

[110] Si osserva in dottrina che su questo profilo la norma stabilisce nei confronti del soggetto interessato un *favor*: cfr. G.M.RICCIO, Data protection officer *e altre figure*, in *La nuova disciplina europea della* privacy, a cura di S. SICA, V. D'ANTONIO e G.M. RICCIO, Padova, 2016, 49 ss.

- *Accountability*;
- nomina DPO nei casi previsti;
- *Privacy by design e Privacy by default*;
- Registro delle attività di trattamento;
- Valutazione di impatto sulla protezione dei dati;
- *Data Breach*;
- Riscontro alle richieste degli interessati.

La violazione del Regolamento può comportare le seguenti sanzioni:

- sanzioni amministrative pecuniarie sino all'importo di 20.000 000 Euro, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (articolo 83, par. 5, lett. b) GDPR);
- risarcimento del danno in favore dell'interessato (articolo 82 GDPR);
- divieto di trattamento dei dati personali fino a che non sia posto rimedio alla situazione di non conformità (articolo 58, par. 2, lett. f) GDPR).

6.3. Il Responsabile del trattamento e il Rappresentante del titolare e del responsabile del trattamento.

Il **Responsabile del trattamento** è definito (con formulazione che riprende quella di cui al D.Lgs. n. 196/2003) come «*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*» (vd. art. 4, n. 8).

Tale figura si presenta come un *alter ego* tecnicamente qualificato del titolare, in quanto dovrebbe fornirgli tutte le informazioni necessarie e assisterlo nelle attività di revisione e di ispezione, segnalandogli l'eventualità che le sue disposizioni violino le norme del Regolamento; un *alter ego* la cui discrezionalità appare tuttavia ridotta, di tipo tecnico professionale ed estrinsecabile attraverso istruttorie per le decisioni del titolare[111]. Il titolare deve in particolare assicurarsi che il responsabile presenti, a norma dell'art. 28, «*garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato*». Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche (così vd. considerando n. 74).

L'art. 28 stabilisce, altresì, che i trattamenti effettuati ad opera del Responsabile del trattamento «*sono disciplinati da un **contratto o da altro atto giuridico** a norma del diritto dell'Unione o degli Stati membri*». Tale atto di designazione, che vincola il responsabile al titolare del trattamento[112],

[111] Così G. COMANDÈ, in *Manuale per il trattamento dei dati personali*, Milano, 2018, 32. *Adde* E.PELINO, *I soggetti del trattamento*, *cit.*, 146 - 147, secondo cui «l'elemento dirimente del ruolo del responsabile consiste nella *strumentalità* rispetto alla finalità decisa dal titolare. Per questa ragione, il responsabile deve attenersi nel trattamento dei dati alle istruzioni del titolare (art. 29), benché, a seconda del tipo di incarico ricevuto o do contratto, possa disporre di un margine discrezionale nella determinazione dei mezzi del trattamento, in base all'interpretazione del Gruppo di lavoro…se il responsabile fuoriesce dall'alveo della strumentalità e usa i dati per finalità e mezzi propri, si colloca *ipso facto* in una posizione assimilata a quella del titolare. La regola trova ora formalizzazione all'art. 28.10».

[112] Cfr. E. PELINO, *I soggetti del trattamento*, cit., 147, il quale precisa che «quale che sia lo strumento di designazione (contratto o altro atto giuridico) è essenziale che esso sia vincolante per il responsabile («*binding on the processor*»). In altre parole, il responsabile non potrà sciogliersi autonomamente dal vincolo, senza sciogliersi, nei casi in cui ciò è possibile, dal sottostante rapporto civilistico o di altro genere con il titolare. Per le stesse ragioni non è perciò legittimo il rifiuto del responsabile di ricevere una designazione che rifletta il rapporto sottostante. L'utilizzo di schemi modello sarà prevedibilmente di notevole aiuto per evitare resistenze pretestuose. La designazione dovrà precedere il compimento di qualsiasi operazione di trattamento da parte del responsabile ed è ragionevole che venga fatta contestualmente alla creazione del rapporto sottostante».

concerne la materia disciplinata, 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. Il Regolamento prescrive un contenuto estremamente dettagliato di quest'atto di designazione, fissandone una serie di **clausole minime inderogabili**[113], stabilendo che il Responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure di sicurezza richieste ai sensi dell'articolo 32;

Si discute sulla possibilità, alla luce del Regolamento di nominare un responsabile interno, secondo la prassi applicativa italiana.

Taluna dottrina, ammette che «Il Rpd può essere, a scelta del titolare/responsabile del trattamento, interno o esterno alla sua organizzazione. Se esterno ci vuole un contratto di servizi stipulato con una persona fisica o giuridica che disciplini i rapporti con il titolare/responsabile del trattamento. Se la funzione di Rpd è svolta da una persona giuridica è indispensabile che ciascun soggetto appartenente al fornitore esterno operante quale Rpd soddisfi tutti i requisiti applicabili come fissati nel Rgpd. È consigliabile, poi, che nel contratto di servizi si preveda che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente. Nel contratto si devono, inoltre, specificare diritti e obblighi dell'impresa da un lato e del Rpd dall'altro» A. CICCIA MESSINA, *Responsabile della protezione dei dati*, in *Dir. e Pratica Lav*., 2017, 42, 2545.

Altra dottrina (cfr. E. PELINO, *I soggetti del trattamento*, *cit.*, 188-149, propende per la soluzione negativa, per una maggiore linearità concettuale (i ruoli subalterni interni sono quelli del personale dipendente (*ex* "incaricati del trattamento") i ruoli subalterni esterni sono quelli dei responsabili del trattamento; l'Autore trae conforto di quest'assunto, da un canto, dall'art. 29 del Regolamento che sembra tracciare una chiara distinzione tra il personale dipendente e le figure del responsabile e del titolare; dall'altro canto, dall'analisi di alcuni degli elementi contrattuali obbligatori dell'atto di designazione, molti dei quali appaiono applicabili esclusivamente a un responsabile esterno, come l'obbligo di informare il titolare dell'esistenza di norme di legge a cui il responsabile è soggetto, ove prevalgano sulle sue istruzioni; l'impegno alla riservatezza dei dipendenti e dei collaboratori, gli obblighi di assistenza di cui alle lettere e) e f) dell'art. 28, che non avrebbe senso specificare nel caso di responsabile interno; l'obbligo di cancellazione o di restituzione dei dati al termine della prestazione del servizio sottostante; il permesso dello svolgimento di attività di ispezione e controllo. Nondimeno, l'Autore non manca di dare atto, in senso contrario, che la definizione di «responsabile» di cui all'art. 4 paragrafo 8) contempla anche il termine «servizio», che appare interpretabile in termini di ripartizione interna. Segnala però che, nella versione inglese si trova il termine «*agency*», dal significato più ampio e conclude che tali spunti testuali non sembrano in definitiva particolarmente significativi.

In una posizione attendista sembra porsi altra dottrina secondo la quale «l'assenza di specifiche in merito all'interno del Regolamento ha sollevato il dubbio circa la compatibilità con il Regolamento medesimo della figura del Responsabile interno. Chi propende per la soluzione negativa sostiene che i ruoli subalterni interni siano unicamente quelli degli incaricati del trattamento, mentre i ruoli subalterni esterni siano quelli dei responsabili del trattamento. Anche l'art. 29 del Regolamento sembra tracciare una precisa distinzione tra il personale dipendente e le figure del Responsabile e del Titolare. Bisogna, però, darsi atto che la definizione di "responsabile" contempla anche il termine "servizio", che potrebbe essere interpretato in termini di ripartizione interna. A ogni modo, questi non sembrano essere elementi particolarmente determinanti per propendere per l'uno o l'altro orientamento. Intanto, diverse Autorità Garanti per la protezione dei dati personali in Europa, tra queste *l'Information Commissioner's Office* (ICO) la *Commission nationale de l'informatique et des libertés* (CNIL), hanno pubblicato documenti e linee guida nei quali escludono la possibilità che il ruolo di Responsabile possa essere affidato a dipendenti del Titolare. L'Italia, dal suo canto, ha sempre ammesso il ruolo del Responsabile interno. Pertanto, sul punto non resta che attendere i possibili futuri orientamenti da parte del Garante Privacy» F. FIORE-M.G. PORTOGALLO, *I gestori del trattamento*, in *Adempimenti privacy per professionisti e aziende*, a cura di C. CARDARELLO-F. D'AMORA-F. FIORE, Milano, 2018, 107 s.

[113] Così E. PELINO, *I soggetti del trattamento*, cit., 145.

d) rispetti le condizioni indicate per ricorrere a un altro responsabile del trattamento;

e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali, dopo che è terminata la prestazione dei servizi relativi al trattamento, e cancelli altresì le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;

h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo, consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da un altro soggetto da questi incaricato.

Il responsabile del trattamento, deve assistere - laddove sia necessario e su richiesta - il titolare del trattamento nel garantire il rispetto degli obblighi derivanti dallo svolgimento di una valutazione d'impatto sulla protezione dei dati nonché dalla previa consultazione dell'autorità di controllo (vd. considerando n. 95).

Altri adempimenti e doveri del Responsabile del trattamento riguardano:

- la tenuta registri trattamenti svolti;
- l'eventuale nomina di un sub-responsabile;
- la nomina DPO laddove ne ricorrano i presupposti indicati dall'art.37;
- la comunicazione al titolare del trattamento;
- obblighi derivanti dal principio di "*Privacy by design e Privacy by default*":
- la segnalazione delle violazioni di dati al alto rischio per i diritti e le libertà degli interessati (la *Data Breach*);
- il riscontro alle richieste degli interessati.

L'art. 28 prevede che il responsabile possa designare direttamente un **altro responsabile (sub - responsabile)**[114] previa autorizzazione scritta, specifica o generale, del titolare del trattamento**.** La norma puntualizza che, in ipotesi di autorizzazione scritta generale, il responsabile del trattamento deve informare il titolare del trattamento di eventuali modifiche previste relative all'aggiunta o alla sostituzione di altri responsabili del trattamento, di guisa che il titolare del trattamento possa valutare l'opportunità di opporsi a tali modifiche. Al sub – responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento, nonché le medesime

[114] Cfr. E. PELINO, *I soggetti del trattamento, cit.*, 151, il quale rimarca come la possibilità della designazione diretta del responsabile da parte di altro responsabile costituisca la novità più significativa introdotta dal Regolamento sull'istituto in esame, osservando come un difetto considerevole dell'articolazione dei ruoli nell'impianto italiano fosse rappresentato proprio dalla necessità che il responsabile fosse sempre designato direttamente dal titolare. Ciò introduceva rigidità non ragionevoli nella modellazione degli schemi di designazione; diversamente – secondo l'Autore – la soluzione fornita dal Regolamento, che si basa sul modello concettuale della delega, fa salvi poteri del titolare ma nello stesso tempo permette flessibilità, consentendo, pur entro i limiti fisati dal titolare, la designazione diretta da responsabile a responsabile.

garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento sia conforme al GDPR. Nondimeno, qualora il sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile (vd. art. 28, par. 4).

Anche il Responsabile del trattamento può essere destinatario delle **sanzioni amministrative**, già previste per il titolare, e risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento, specificatamente diretti ai responsabili del trattamento, oppure se ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento (vd. art. 82).

Il Responsabile, laddove abbia pagato l'intero risarcimento del danno, ha il **diritto di regresso** in relazione alla responsabilità degli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento.

L'art. 27 prescrive che, qualora il GDPR sia applicabile anche a Titolari o Responsabili del trattamento non stabiliti nell'UE ai sensi dell'articolo 3, par.2, questi ultimi debbano designare per iscritto un **Rappresentante del titolare o del responsabile nell'Unione**. Si tratta di un mandatario nell'Unione del titolare o del responsabile stabiliti extra UE, il cui incarico copre ogni questione che importi obblighi in capo al mandante ai sensi del regolamento (art. 4, paragrafo 17)[115].

L'obbligo di designare tale Rappresentante non sussiste, per espressa previsione dell'art. 27, laddove:

- il trattamento sia occasionale oppure non coinvolga, su larga scala, le categorie particolari di dati di cui all'articolo 9, paragrafo 1, o di giudiziali di cui all'art. 10, ed è improbabile che presenti un rischio per i diritti e le libertà delle persone fisiche, tenuto conto della natura, del contesto, dell'ambito di applicazione e delle finalità del trattamento;

- il mandante sia un'autorità pubblica o un organismo pubblico.

La mancata osservanza delle prescrizioni contenute nel paragrafo 1 dell'art. 37, relative all'obbligo di designazione del DPO, può comportare:

- sanzioni amministrative pecuniarie sino all'importo di 10.000 000 Euro, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (articolo 83, par. 4, lett. a) GDPR);

- il risarcimento del danno in favore dell'interessato (articolo 82 GDPR);

[115] Così si esprime E. PELINO, *I soggetti del trattamento, cit.*, 152, il quale chiarisce come la figura del rappresentante era contemplata nella direttiva 95/46 e nel codice privacy, ma le funzioni e il ruolo non erano adeguatamente mesi a fuoco. Il Regolamento ha precisato alcuni profili della disciplina, ampliandone l'applicazione e introducendo la figura del rappresentante del responsabile. Osserva, inoltre, che l'ambito applicativo dell'istituto è più ristretto rispetto a quello designato dall'art. 3.2 del Regolamento, per cui si darà il caso di titolari o responsabili non stabiliti nell'Unione e privi di rappresentante nella stessa ai quali risulta tuttavia applicabile la disciplina del Regolamento. La *ratio* dell'istituto appare quella di creare, nei casi di più intensa rilevanza dei profili di rischio del trattamento, un elemento di prossimità agli interessati e alle Autorità garanti europee con cui relazionarsi e al quale indirizzare pretese giuridiche anche in sostituzione del titolare o del responsabile quando questi sono stabiliti in Paesi terzi. Ancora su questa figura, l'Autore in discorso (vd. pag. 159) osserva criticamente come il Regolamento non abbia previsto misure sanzionatorie nei confronti del rappresentante, lamentando l'incoerenza della creazione di una figura destinataria di istanza ma non sanzionabile ove le disattenda.

- il divieto di trattamento dei dati personali fino a che non sia posto rimedio alla situazione di non conformità (articolo 58, par. 2, lett. f) GDPR).

6.4. Il Responsabile della protezione dati (DPO).

Una delle maggiori novità introdotte dal G.D.P.R. riguarda il **Responsabile della protezione dei dati**, nuova figura[116] che si affianca al titolare del trattamento, al Responsabile del trattamento e agli Interessati, significativamente descritta in dottrina quale «primo difensore del dato e non solo responsabile per le eventuali violazioni su di esso, come era nel vecchio sistema, visto che deve essere in possesso di specifici requisiti, quali la competenza, l'esperienza, l'indipendenza e l'autonomia delle risorse»[117].

È obbligatoria la nomina del DPO, ove sussistano i presupposti indicati dall'art. 37[118], ma ne è possibile la designazione su base volontaria.

In dettaglio, l'art. 37 prescrive che «*il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:*

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

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

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

Si tratta di una figura di **garanzia e indipendenza,** che non deve essere in conflitto di interesse con il titolare o con il responsabile del trattamento. Proprio a garanzia della sua indipendenza, il titolare e il responsabile del trattamento si assicurano che egli non riceva alcuna istruzione per quanto riguarda l'esecuzione dei suoi compiti. È inoltre *expressis verbis* sancito che il DPO non possa essere rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti e che egli riferisca direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento. Questi ultimi, peraltro, devono assicurare che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali; devono altresì sostenerlo nell'esecuzione dei suoi compiti, fornendogli le risorse necessarie per assolvere gli stessi, per accedere ai dati personali e ai trattamenti, nonché per preservare la propria conoscenza specialistica (vd. art. 38).

---

[116] Per una concisa indagine sulla introduzione della figura del DPO, anche di ordine comparatistico, cfr.. G.M. RICCIO, Data protection officer *e altre figure,* in *La nuova disciplina europea della* privacy, a cura di S. SICA, V. D'ANTONIO e G.M. RICCIO, Padova, 2016, 49 ss.

[117] Così G. PALAZZOLO, *La banca dati e le sue implicazioni civilistiche in tema di cessione e deposito alla luce del reg. (ue) n. 2016/679*, in *Contr. e Impr*., 2017, 2, 613.

[118] G.M. RICCIO, Data protection officer *e altre figure*, cit., 52, osserva come l'obbligo di designazione di tale figura sia imposto solo per le grandi società, o meglio, per le società he trattano una mole significativa di dati personali o di dati rientranti nel cd. "nocciolo duro" della *privacy*. La manata estensione a tutte le società risponde all'esigenza, da un lato, di non "volgarizzare" questa qualifica che dovrebbe competere esclusivamente a professionisti che vantano una radicata esperienza nel settore e, dall'altro (e soprattutto), dalla necessità di non gravare le imprese on costi eccessivi.

Il DPO è designato[119] in funzione delle sue qualità professionali, le quali devono essere adeguate alla complessità dei trattamenti di dati posti in essere dall'azienda: a tal fine, deve essere selezionato tra figure con competenze tecnico-legali e con esperienza in materia di protezione dei dati.

Svolge, in linea generale, un ruolo misto di vigilanza dei processi interni alla struttura del titolare e del responsabile, di consulenza per costoro, di contatto rispetto agli interessati e alle Autorità garanti[120]. In particolare, i suoi **compiti sono molteplici** e possono distinguersi in compiti di natura consultiva, formativa, di garanzia e di "punto di contatto". In dettaglio, l'art. 39 prevede compiti specifici che costituiscono il contenuto minimo delle attività del DPO, potendosi queste declinare ed esplicare in altri modi all'interno della struttura organizzativa del titolare e del responsabile del trattamento[121].

In dettaglio, il DPO, secondo la norma testé richiamata, «è incaricato almeno dei seguenti compiti», ai quali deve attendere considerando debitamente i rischi inerenti al trattamento, in ragione della natura, dell'ambito applicativo, del contesto e delle finalità del medesimo. In dettaglio egli:

a) informa e fornisce consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla materia della protezione dei dati;

b) sorveglia l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e ne sorveglia lo svolgimento;

d) coopera con l'autorità di controllo;

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

Le sanzioni previste riguardano:

---

[119] *Adde*, diffusamente, A. CICCIA MESSINA, *Responsabile della protezione dei dati*, in *Dir. e Pratica Lav*., 2017, 42, 2545, il quale ammette «la designazione congiunta da parte di più entità giuridiche, ad esempio un gruppo imprenditoriale può nominare un unico Rpd. Questo vale anche per le pubbliche amministrazioni. In ogni caso il Rpd deve essere in grado di svolgere le sue mansioni in maniera efficiente, soprattutto quando lavora per più committenti. In caso di designazione congiunta il Rpd deve comunque essere "facilmente raggiungibile" da ciascuna sede. Facile raggiungibilità significa prontezza della possibilità di comunicazione da parte degli interessati, dell'autorità di controllo e dei soggetti interni all'organismo o all'ente: tutti devono poter rintracciare il Rpd senza difficoltà e senza perdita di tempo. Ciò sia con la presenza fisica sia con l'immediato collegamento a distanza, con una linea dedicata o con mezzi equivalenti. Il Rpd deve avere, se necessario, una sua organizzazione che lo supporti e le comunicazioni devono avvenire nella lingua utilizzata dalle autorità di controllo e dagli interessati».

[120] Così E. PELINO, *I soggetti del trattamento*, cit., 163. *Adde*, sul duplice ruolo consultivo e di raccordo del D.P.O. M. GAGLIARDI, in *Manuale per il trattamento dei dati personali*, a cura di G. COMANDÈ e G. MALGIERI, Milano, 2018, 11 ss.

[121] In tali termini vd. M.GAGLIARDI, *op.cit.*, 16.

- sanzioni amministrative pecuniarie sino all'importo di 10.000 000 Euro, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (articolo 83 (4) (a) GDPR);

- il risarcimento del danno in favore dell'interessato (articolo 82 GDPR).

7. Rischio e responsabilizzazione.

La descrizione del Regolamento fin qui condotta ha lasciato intravedere quanto l'intera struttura normativa sia permeata dal cd "*risk-based approach*", richiedendosi ai titolari del trattamento «valutare le proprie attività di trattamento in ottica *risk based*, in maniera tale da indirizzare coerentemente le proprie scelte tecniche ed organizzative»[122].

Questa endiade "rischio-responsabilizzazione" esce oltremodo confermata laddove l'angolo visuale dell'interprete si appunti proprio sugli specifici obblighi ed adempimenti che devono essere curati. Oltre a quelli fin qui già descritti [(come, tra l'altro, l'informativa (artt. 13 e 14); l'adozione di misure tecniche e organizzative adeguate per garantire un livello adeguato di sicurezza ai rischi (art. 32); la designazione del Responsabile della protezione dei dati (art. 37)], bisogna trattare a questo punto gli adempimenti relativi alla:

- adozione di misure tecniche e organizzative adeguate (art. 24);
- protezione dei dati fin dalla progettazione e protezione per impostazione definita (art. 25); designazione di un rappresentante nell'Unione (art. 27);
- notifica all'autorità di controllo o all'interessato in caso di violazioni di dati personali (artt. 33-34);
- una valutazione d'impatto sulla protezione dei dati prima di iniziare il trattamento (art. 35).
- tenuta di un registro per le attività di trattamento (artt. 30-31).

7.1. A*ccountability*.

Una delle maggiori novità del Regolamento è costituita dal principio di *accountability*, in forza del quale viene affidato ai titolari del trattamento il compito di «mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al (...) regolamento» (art. 24)[123]. Ne discende quindi che grava sul titolare del trattamento il dovere di valutare le misure tecniche e organizzative da adottare sulla base della natura dei dati, dell'oggetto, delle finalità di trattamento. Si tratta di misure non soltanto tecnologiche ma anche organizzative, dal momento che l'unico modo efficace di affrontare il problema della sicurezza dell'informazione è quello che ne comporta una visione integrata: informatica, giuridica e organizzativa»[124].

---

[122] M. GAGLIARDI, *Gli adempimenti previsti dal Regolamento: quadro generale, i registri*, in *Manuale per il trattamento dei dati personali*, a cura di G. COMANDÈ e G. MALGIERI, Milano, 2018, 63 ss.

[123] «Quello di *accountability* è un concetto difficilmente traducibile in una parola della nostra lingua e reso, nella versione italiana del regolamento, con il termine "responsabilità". In realtà, esso si colloca a metà tra la responsabilità e la *compliance*, perché il titolare deve essere *compliant* rispetto alla normativa in esame. Bisognerà trovare un termine diverso o composto per evitare l'utilizzo del termine "responsabilità": problemi di traduzione esistono, ogni lingua ha dei termini difficilmente traducibili e quello dell'*accountability* appare proprio uno di questi casi. In materia di tutela dei diritti della personalità, questo principio potrebbe apparire come un corollario del principio di trasparenza. Tuttavia, l'*accountability* dev'essere intesa non già come completa accessibilità, da parte dell'interessato, alle informazioni circa l'attività di un dato operatore, bensì come garanzia della conformità di tale attività alla disciplina di settore: conformità che l'operatore - il titolare del trattamento - dev'essere in grado di dimostrare in qualsiasi momento» E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contr. e impr*., 2018, 120 s.

[124] G. FINOCCHIARO, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuove Leggi Civ. Comm*., 2017, 1, 1. Ivi, si richiama anche Il Gruppo di lavoro articolo 29 per la protezione dei dati, il quale ha esaminato

7.2. *Privacy by design* e *by default.*

Nel mettere in atto le predette misure il titolare del trattamento deve tenere presenti due importanti principi:

- il principio della *privacy by design*, in base al quale bisogna garantire la protezione dei dati sin dalla progettazione[125]

- il principio della *privacy by default*, in base al quale bisogna garantire che i dati vengano raccolti nella minore misura possibile e nel rispetto delle finalità del trattamento[126].

Entrambi i principi, enunciati nei "Considerando", sono contenuti nell'art. 25 del Regolamento, mentre l'art. 42 ammette che il titolare potrà servirsi di un meccanismo di certificazione *ex* art. 42 come elemento per dimostrare la conformità del trattamento ai predetti principi[127].

7.3. *Data breach notification.*

---

l'approccio alla protezione dei dati basato sul principio dell'*accountability* nel parere 3/2010. Secondo il Gruppo di lavoro articolo 29 per la protezione dei dati, due sono gli elementi principali: "(i) la necessità che il responsabile (N.d.A.: titolare) del trattamento adotti misure appropriate ed efficaci per attuare i principi di protezione dei dati; (ii) la necessità di dimostrare, su richiesta, che sono state adottate misure appropriate ed efficaci. Pertanto, il responsabile (N.d.A.: titolare) del trattamento deve fornire la prova di quanto esposto al punto (i)".

[125] Occorre «in altre parole, che qualsiasi progetto debba essere realizzato avendo presente, sin dal principio - *by design*, appunto - la riservatezza dell'utente finale e la protezione dei suoi dati personali, con tutte le necessarie applicazioni di supporto (informatiche e non). Si tratta di un approccio sempre più utilizzato al problema della protezione dei dati, volto a garantire la migliore operatività possibile della protezione» E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contr. e impr*., 2018, 122 s.. In termini di "approcci non reattivi ma proattivi alla circolazione dei dati personali, come la *privacy by design*" si esprime F. PIRAINO, *Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove Leggi Civ. Comm*., 2017, 2, 388. A questo l'Autore associa la regola della *privacy by default*.

[126] «Si tratta, in altre parole, della summa dei principi di "minimizzazione dei dati" e di "limitazione della finalità" (da cui discende a sua volta il principio della "limitazione della conservazione", il quale impone di limitare nel tempo quanto più possibile il trattamento e l'archiviazione dei dati raccolti)» E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contr. e impr*., 2018, 122 s..

[127] «I principi della *privacy by default* e *by design* ruotano anche essi attorno all'approccio basato sul rischio e sull'assunzione di responsabilità» e «sono specificazioni di principi generali come il principio di minimizzazione dei dati personali che dovrebbero essere utilizzati se non diversamente possibile. Tuttavia questi due principi nell'economia del Regolamento assumono una valenza particolare, generalizzando la *privacy by default* in principio per cui il livello di base di protezione fissato in un tratto (e di conseguenza nell'uso delle tecnologie che lo rendono possibile) deve essere quello più elevato possibile che non impedisca la funzionalità del trattamento; mentre il principio della *privacy by design* impone di considerare le opzioni possibili e necessarie già in fase di disegno del trattamento e dunque di incorporare sin dall'inizio i principi di tutela previsti dal regolamento» G. COMANDÈ, *Il diritto di ricevere informazioni e il diritto d'accesso*, in *Manuale per il trattamento dei dati personali*, cit., 79.

Significativo criterio ermeneutico di orientamento in materia anche *Considerando* 78: «La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default. Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare 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. 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 produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici».

Tutti i titolari hanno **l'obbligo di notificare all'Autorità Garante e all'interessato che sia avvenuta una violazione dei dati personali** (artt. 33 e 34).

Per violazione dei dati personali si intende, in base all'art. 4 del regolamento, "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"[128].

La prima notifica ha per destinatario l'Autorità di controllo e deve essere effettuata **senza ingiustificato ritardo e, ove possibile, entro 72 ore** dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo (art. 33).

La seconda notifica è indirizzata **senza ingiustificato ritardo** all'interessato quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche (art. 34). Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

a) 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;

b) 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 di cui al paragrafo 1;

c) 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[129].

Oltre alla notifica, il titolare del trattamento è tenuto a registrare e documentare qualsiasi violazione dei dati personali, compresi i dettagli e le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

7.4. *Data protection impact assessment.*

Un ulteriore strumento di responsabilizzazione, al contempo, elemento di valutazione per dimostrare di aver rispettato la disciplina fissata dal Regolamento è la c.d. *Valutazione d'impatto*

[128] «La violazione, dunque, può ricorrere a causa di eventi imprevisti (calamità naturali, incendi, etc.) o dipendere dall'attività umana, sia essa intenzionale o di natura meramente colposa, comportando differenti lesioni dei diritti degli interessati, con conseguenti danni di natura materiale o immateriale» S. VIGLIAR, Data breach *e sicurezza informatica*, in *La nuova disciplina europea della* privacy, a cura di S. SICA-V. D'ANTONIO-G.M. RICCIO, Padova, 2016, 241. Ivi, per richiami e riferimenti al *Considerando* 85 del Regolamento nonché per richiami al maggiore numero di episodi *Data breach*: attacchi per mezzo di applicazioni *on-line*; intrusioni nei punti vendita; utilizzo abusivo di informazioni riservate; errore; furto e perdita; *crimeware*; *skimming*; spionaggio informatico; interruzione del servizio.

[129] Per ulteriori approfondimenti del tema si fa rinvio alle linee guida del Gruppo di lavoro Art. 29 per la protezione dei dati - *Guidelines on Personal data breach notification under Regulation 2016/679, WP 250 rev1*-Ottobre 2017, modificate il 6 Febbraio 2018 disponibili a *http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052*. Ivi, tra l'altro, si definiscono le nozioni di: "distruzione", "danno", trattamento non autorizzato illecito". Si entra nel merito delle violazioni, suddividendole per casi e ipotesi; sulle conseguenze dipendenti da una violazione non affrontata in modo adeguato e tempestivo (*Considerando* 85); sulle sanzioni.

privacy, ossia la valutazione del rischio inerente al trattamento. In base agli artt. 35 e 36 del Regolamento il titolare è tenuto ad effettuare una valutazione di impatto **prima dell'avvio del trattamento**, quando un tipo di trattamento, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare **un rischio elevato (per gravità e probabilità del suo verificarsi) per i diritti e le libertà delle persone fisiche**. Nel farlo, il titolare del trattamento si consulta con il responsabile della protezione dei dati, qualora ne sia designato. Quest'ultimo fornirà la sua consulenza, ma non sarà suo il compito di condurre la valutazione, che resta in capo al titolare del trattamento. Allo stesso modo, il titolare del trattamento consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio. L'oggetto per la valutazione d'impatto può essere un singolo trattamento oppure più trattamenti purché simili tra loro per natura, ambito di applicazione, contesto, finalità e rischi.

Il Regolamento offre poi delle utili indicazioni riguardo ai trattamenti assoggetti a tale obbligo e quelli invece esclusi.

La valutazione d'impatto sulla protezione dei dati è richiesta in particolare nei casi seguenti di:

a) 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) trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o

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

La valutazione d'impatto sulla protezione dei dati non è richiesta in particolare nei casi seguenti per i trattamenti:

- che non presentano un rischio elevato;

- che trovano il proprio fondamento in una disposizione normativa di uno Stato Membro o del diritto dell'Unione;

- in corso al 25 maggio 2018 che siano già stati autorizzati dalle autorità competenti e non presentino variazioni significative prima di tale data;

- che siano stati oggetto di una valutazione d'impatto per una molteplicità di trattamenti simili;

- che sia incluso nella lista dei trattamenti esclusi espressamente dalle autorità di controllo.

Quanto ai caratteri della valutazione, l'art. 35 precisa che quest'ultima deve contenere almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione[130].

8. Il registro generale delle attività di trattamento svolte sul dato personale del trattato.

Infine, tra le principali novità, vi è l'obbligo di tenuta di un Registro generale delle attività di trattamento svolte sul dato personale del trattato. Si tratta di uno strumento di responsabilizzazione per il titolare ed il responsabile del trattamento, nonché uno strumento di controllo successivo da parte dell'Autorità di controllo (art. 58) riguardo al rispetto della normativa da parte dei soggetti obbligati (art. 30).

In base al paragrafo 5 dell'art. 30 non sono obbligate alla sua tenuta le imprese o organizzazioni con meno di 250 dipendenti, a meno che:

- il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato;

- il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10[131].

---

[130] Sul soggetto tenuto, sui criteri identificativi, sui termini di effettuazione (quanto più a monte possibile nelle fasi di progettazione del trattamento, sui soggetti coinvolti nello svolgimento della valutazione nonché sul contenuto e sulle modalità di svolgimento, G. MALGIERI, *La valutazione d'impatto sulla protezione dei dati personali (DPIA)*, in *Manuale per il trattamento dei dati personali*, G. COMANDÈ e G. MALGIERI, Milano, 2018, 70 ss. Su quest'ultimo aspetto, molte sono le opzioni disponibili. A tal fine, costituiscono una utile bussola di orientamento le linee guida esplicative del Gruppo dei garanti europei "Articolo 29" (c.d. WP29), del 2017. In essa si precisa che quando si prevede di effettuare un trattamento che possa presentare un rischio elevato, il titolare del trattamento deve «scegliere una metodologia per la valutazione d'impatto sulla protezione dei dati (esempi riportati nell'allegato 1) che soddisfi i criteri di cui all'allegato 2, oppure specificare ed attuare un processo sistematico di valutazione d'impatto sulla protezione dei dati che:

- sia conforme ai criteri di cui all'allegato 2;
- sia integrata nei processi in materia di progettazione, sviluppo, cambiamento, rischio e riesame operativo in conformità con i processi, il contesto e la cultura interni;
- coinvolga le parti interessate appropriate e definisca chiaramente le loro responsabilità (titolare del trattamento, responsabile della protezione dei dati, interessati o loro rappresentanti, imprese, servizi tecnici, responsabili del trattamento, responsabile della sicurezza dei sistemi d'informazione, ecc.);
- fornire la relazione relativa alla valutazione d'impatto sulla protezione dei dati all'autorità di controllo, laddove gli venga richiesto di procedere in tal senso;
- consultare l'autorità di controllo, qualora il titolare del trattamento non sia riuscito a determinare misure sufficienti per attenuare i rischi elevati;
- riesaminare periodicamente la valutazione d'impatto sulla protezione dei dati e il trattamento che essa valuta, almeno quando si registra una variazione del rischio posto dal trattamento;
- documentare le decisioni prese».

Così, **Gruppo di lavoro Art. 29 per la protezione dei dati**, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679, 2017*, disponibile su http*://www.garanteprivacy.it/regolamentoue/DPIA*. Sul punto, e per approfondimenti, M. SOFFIENTINI, *Nuovi comportamenti per la compliance aziendale della privacy*, in *Dir. e Pratica Lav*., 2017, 41, 2453.

[131] In definitiva, «l'obbligo di tenuta dei registri dei trattamenti, lungi dall'essere un adempimento burocratico privo di utilità, se bene inserito nel contesto delle attività di gestione dei trattamenti può rivelarsi funzionale alla migliore conoscenza delle attività di trattamento ed alla corretta gestione dei vari adempimenti prescritti dal Regolamento. Inoltre, è bene rammentare che dai registri in parola si parte per la conoscenza delle attività di un titolare da questi si prendono le mosse per tutte le valutazioni richieste al titolare» M. GAGLIARDI, *Il nuovo obbligo di tenuta del registro delle attività di trattamento di dati personali*, in *Manuale per il trattamento dei dati personali*, G. COMANDÈ e G.

La finalità della previsione di un siffatto Registro è evidente: consentire «al titolare e all'autorità di controllo, su richiesta, di disporre di un quadro complessivo dei trattamenti di dati personali svolti dallo specifico soggetto. In quanto tale, esso costituisce un presupposto indispensabile ai fini dell'osservanza delle norme e, pertanto, un'efficace misura di responsabilizzazione»[132].

Per quanto riguardo la forma, esso deve essere tenuto in forma scritta o in formato elettronico. Deve essere manutenuto e aggiornato per garantire una effettiva corrispondenza alla realtà dei trattamenti.

Riguardo poi al contenuto del Registro bisogna distinguere fra il Registro del titolare del trattamento (e, ove applicabile, il suo rappresentante) e il Registro del responsabile del trattamento (e, ove applicabile, il suo rappresentante).

Il Registro del titolare del trattamento contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

b) le finalità del trattamento;

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 od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Il Registro del responsabile del trattamento contiene:

a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del

---

MALGIERI, Milano, 2018, 66. Infine, si osserva che, anche se l'obbligo di tenuta non riguarda le imprese o le organizzazioni con meno di 250 dipendenti, tuttavia, «sarebbe bene che anche queste li avessero, almeno per grandi linee, in quanto l'eccezione non si applica se i trattamenti da loro effettuati possono presentare rischi per i diritti e le libertà degli interessati, se i trattamenti non siano occasionali e se riguardino le categorie particolari di dati di cui agli artt. 9 e 10. Dunque, le imprese interessate devono comune essere in grado di valutare se e quali rischi riguardino i trattamenti di dati effettuati, e soprattutto devono essere consapevoli delle categorie di dati trattati e dell'occasionalità o ricorrenza/sistematicità dei trattamenti stessi. Per questa ragione si ritiene che la tenuta di un registro, anche in forma semplificata, possa aiutare a tenere monitorati questi fattori, anche in vista di un eventuale passaggio al regime dell'obbligo di tenuta dei registri» (ivi, 66 s.).

[132] M. SOFFIENTINI, *Nuovi comportamenti per la compliance aziendale della privacy*, in *Dir. e Pratica Lav*., 2017, 41, 2453. Cfr., G. PALAZZOLO, *La banca dati e le sue implicazioni civilistiche in tema di cessione e deposito alla luce del reg. (ue) n. 2016/679*, in *Contr. e impr*., 2017, 2, 613.

titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;

b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

9. Codici di condotta e certificazioni.

Enunciati descrittivamente, per caratteri e funzione, nei Considerando 98[133] e 99[134], i Codici di condotta costituiscono un'altra importante novità introdotta dal GDPR, testualmente contenuta nell'art 40 e nell'art. 24, paragrafo 3 (dove l'adesione ad essi come a un meccanismo di certificazione può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento[135]).

La loro funzione è molteplice.

Per un verso, «i codici rafforzeranno il principio di responsabilizzazione, "avvicinando" la normativa a titolari e responsabili di settori/ambiti specifici e rendendone le attività di trattamento ancora meglio verificabili».

Peraltro, «essi semplificheranno il rispetto in concreto del GDPR: i loro contenuti forniranno indicazioni pratiche su come mettere in atto (e poi dimostrare di avere messo in atto) le misure e gli obblighi previsti dal RGPD»[136].

Infine, questa «adesione a codici di condotta fornisce prova dell'ottemperanza agli obblighi del Regolamento ed è un elemento valutato positivamente in termini di *Impact Assessment*. Secondo alcuni Autori, l'adesione potrebbe, peraltro, nella denegata ipotesi di mancato rispetto di qualche obbligo da parte dell'organizzazione aderente al codice di condotta, influire sulla determinazione delle sanzioni in termini di attenuazione»[137].

---

[133] *Considerando* 98 «Le associazioni o altre organizzazioni rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento dovrebbero essere incoraggiate a elaborare codici di condotta, nei limiti del presente regolamento, in modo da facilitarne l'effettiva applicazione, tenendo conto delle caratteristiche specifiche dei trattamenti effettuati in alcuni settori e delle esigenze specifiche delle microimprese e delle piccole e medie imprese. In particolare, tali codici di condotta potrebbero calibrare gli obblighi dei titolari del trattamento e dei responsabili del trattamento, tenuto conto del potenziale rischio del trattamento per i diritti e le libertà delle persone fisiche».

[134] *Considerando* 99 «Nell'elaborare un codice di condotta, o nel modificare o prorogare tale codice, le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento dovrebbero consultare le parti interessate pertinenti, compresi, quando possibile, gli interessati, e tener conto delle osservazioni ricevute e delle opinioni espresse in riscontro a tali consultazioni».

[135] Come rileva attenta dottrina, oltre all'art. 24, paragrafo 3, sono molti i riferimenti normativi contenuti nel Regolamento ispirati al principio di responsabilizzazione, inteso come capacità di dimostrare la conformità alle prescrizioni del Regolamento. A tal fine, si fa richiamo agli artt. 28 paragrafo 5, 32, paragrafo 3, 35, paragrafo 8, 46, paragrafo 2. Cfr., L. BOLOGNINI, *Codici di condotta*, in *Il regolamento privacy europeo*, cit., 422.

[136] L. BOLOGNINI, *Codici di condotta*, in *Il regolamento privacy europeo*, cit., 433.

[137] Così, D. AMRAM, *Codici di condotta*, in *Manuale per il trattamento dei dati personali*, G. COMANDÈ e G. MALGIERI, Milano, 2018, 105.

In base all'art. 40 GDPR, l'oggetto dei codici di condotta può riguardare i seguenti aspetti:

a) il trattamento corretto e trasparente dei dati;
b) i legittimi interessi perseguiti in contesti specifici;
c) la raccolta dei dai personali;
d) la pseudonimizzazione dei dati personali;
e) l'informativa al pubblico e agli Interessati;
f) l'esercizio dei diritti degli Interessati;
g) l'informativa da rendere ai minori e la loro protezione, nonché le modalità con cui ottenere il consenso di chi esercita la potestà genitoriale sul minore;
h) le misure e le procedure per la responsabilizzazione e la protezione dei dati fin dalla progettazione e per impostazione predefinita (articoli 24 e 25 GDPR, nonché le misure volte a garantire la sicurezza del trattamento (articolo 32 GDPR);
i) la notifica di una violazione di dati personali all'autorità di controllo e la comunicazione di tale violazione agli Interessati;
j) il trasferimento dei dati personali verso paesi terzi o organizzazioni internazionali;
k) le procedure stragiudiziali e di altro tipo per comporre le controversie tra Titolari del trattamento e Interessati[138].

Una volta elaborato, il progetto del codice di condotta deve essere sottoposto all'Autorità di controllo chiamata ad esprimere un parere. Nel fare ciò, l'autorità di controllo esamina il progetto, per verificare se è conforme al GDPR e se offre garanzie adeguate. In caso di esito positivo, il codice di controllo è registrato e pubblicato. Laddove, poi, il codice di condotta riguardi attività di trattamento che coinvolgono diversi Stati membri, si rende necessario anche l'esame da parte del Comitato europeo per la protezione dei dati. Quest'ultimo, valutato il codice, la sua conformità al GDPR e la presenza di garanzie adeguate, trasmette il suo parere alla Commissione Europea. Quest'ultima potrà decidere se il codice, la sua modifica o proroga possano avere validità generale nell'Unione Europea. In caso di esito positivo, la Commissione provvede ad attribuire validità generale al codice. La Commissione provvede a dare un'adeguata pubblicità dei codici approvati per i quali vi è stato il riconoscimento della predetta validità generale. Il Comitato raccoglie in un registro tutti i codici di condotta, le modifiche e le proroghe dei codici approvati e li rende pubblici.

Altro strumento attraverso il quale il titolare del trattamento può dimostrare l'osservanza delle prescrizioni del GDPR[139] è costituito dalla adesione a meccanismi volontari di certificazione e sigilli nonché marchi di protezione dei dati[140].

Questi meccanismi, descrittivamente enunciati nel Considerando 100[141], sono introdotti e disciplinati dagli art. 42 e 43 del Regolamento[142]. La loro funzione è quella di consentire

[138] «(…) non si tratta di un elenco esaustivo né chiuso, dal momento che, (…), le attività di promozione rispetto all'adozione dei codici possono essere portate avanti dalle DPA, dal comitato e dalla Commissione in qualsiasi momento e senza limite di ambito, oggetto o settore» L. BOLOGNINI, *Codici di condotta*, in *Il regolamento privacy europeo*, cit., 422.

[139] «Essi hanno lo scopo, soprattutto, se adottati a livello dell'UE e non solo nazionale, di dimostrare la conformità al RGPD dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento, ma sono ovviamente procedure volontarie (cfr. art. 42.3), non obblighi, e non è necessario possedere un marchio per far sì che il trattamento possa essere legittimamente effettuato» C. BISTOLFI, *Certificazione*, in *Il regolamento privacy europeo*, cit., 438. Ivi per approfondimenti in tema di rilascio della certificazione, dell'organismo di certificazione e dei criteri per l'accreditamento degli organismi di certificazione.

[140] «Un'impresa certificata ai sensi dell'art. 42 del Regolamento semplifica la dimostrazione del rispetto della normativa sui dati personali di cui all'art. 24, l'utilizzazione di tecniche di *privacy by design* e *privacy by default* di cui all'art. 25, nonché l'adozione di misure adeguate di sicurezza del trattamento di cui all'art. 32» D. AMRAM, *Codici di condotta*, in *Manuale per il trattamento dei dati personali*, G. COMANDÈ e G. MALGIERI, Milano, 2018, 107.

all'interessato di valutare se «l'impresa che offre un determinato prodotto/servizio adotti o meno tutte le misure a garanzia della protezione dei dati personali: si tratta di consentire agli interessati di comprendere il livello di rispetto dei principi e degli obblighi imposti dal Regolamento da parte dell'impresa c.d. certificata»[143].

10. I poteri delle Autorità di controllo.

Nel fare fronte ad una esigenza di «definizione delle tutele esperibili e di garanzia sul controllo sulla corretta applicazione dei principi in materia di tutela dei dati sensibili e personali»[144], il legislatore europeo ha inteso approntare una disciplina uniforme fondata su un modello accentrato di controllo, incardinato in diversi organismi di rilievo ora nazionale ora transazione: più comunemente noti come Autorità di controllo[145].

L'art. 51 del Regolamento prevede infatti l'istituzione da parte di ogni Stato membro di «una o più autorità pubbliche indipendenti (…) incaricate di sorvegliare l'applicazione del presente 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 (l'«autorità di controllo» (par. 1). Ciascuna Autorità di controllo «contribuisce alla coerente applicazione del presente regolamento in tutta l'Unione» (par. 2) e a tal fine tutte «cooperano tra loro e con la Commissione» (par. 2). Laddove, poi, «in uno Stato membro siano istituite più autorità di controllo, detto Stato membro designa l'autorità di controllo che rappresenta tali autorità nel comitato e stabilisce il meccanismo in base al quale le altre autorità si conformano alle norme relative al meccanismo di coerenza di cui all'articolo 63» (par. 3).

Le **funzioni** delle Autorità di Controllo, in base al *Considerando* 122[146] e all'art. 55 del Regolamento, possono essere distinte in funzioni di: controllo; promozionali, consultive; gestionali; di collaborazione finalizzata alla protezione dei dati personali[147].

---

[141] *Considerando* 100: «Al fine di migliorare la trasparenza e il rispetto del presente regolamento dovrebbe essere incoraggiata l'istituzione di meccanismi di certificazione e sigilli nonché marchi di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi».

[142] «Nell'impianto normativo disegnato dal legislatore UE, codici di condotta e certificazioni – in quanto relativi alla materia dei trattamenti dei dati personali – vedono limate le differenze, per la semplice ragione che le conformità ai codici di condotta divengono oggetto di monitoraggio da parte di appositi organismi terzi, ovvero cessano di essere autoreferenziali» T. GUIDA, *I codici di condotta (artt. 40-43)*, in *Adempimenti privacy per professionisti e aziende*, cit., 144 s.

Volendo coglierne una differenza, si può «precisare che, mentre i codici di condotta, in termini di "garanzie adeguate", valgono anche come riferimento per la valutazione di impatto (DPIA), le certificazioni non sono previste dall'art. 35; esse sono, viceversa, considerate da sole nel caso peculiare di cui all'art. 25.3 relativo alla *data protection-by design* e *by default* (…) e in quello dell'art. 28.6» C. BISTOLFI, *Certificazione*, in *Il regolamento privacy europeo*, cit., 441.

[143] D. AMRAM, *Codici di condotta*, in *Manuale per il trattamento dei dati personali*, cit., 106. Ivi, per riferimenti ai rischi connessi al trattamento dei dati, cfr. *Considerando* 75, mentre con riferimento alla incidenza dei codici di contratta e delle certificazioni sul computo della responsabilità del titolare del trattamento, cfr. *Considerando* 77, 81, 100 nonché art. 24, paragrafo 3.

[144] F. FRENI, *Le* Authorities, in *Adempimenti privacy per professionisti e aziende*, cit., 167.

[145] *Considerando* 129: «Le autorità di controllo dovrebbero controllare l'applicazione delle disposizioni del presente regolamento e contribuire alla sua coerente applicazione in tutta l'Unione, così da tutelare le persone fisiche in relazione al trattamento dei loro dati personali e facilitare la libera circolazione di tali dati nel mercato interno. A tal fine, le autorità di controllo dovrebbero cooperare tra loro e con la Commissione, senza che siano necessari accordi tra gli Stati membri sulla mutua assistenza o su tale tipo di cooperazione».

[146] *Considerando* 122: «Ogni autorità di controllo dovrebbe avere la competenza, nel territorio del proprio Stato membro, a esercitare i poteri e ad assolvere i compiti a essa attribuiti a norma del presente regolamento. Ciò dovrebbe comprendere in particolare il trattamento nell'ambito delle attività di uno stabilimento del titolare del trattamento o del responsabile del trattamento sul territorio del proprio Stato membro, il trattamento di dati personali effettuato dalle pubbliche autorità o dagli organismi privati che agiscono nel pubblico interesse, il trattamento riguardante gli interessati

I **poteri** delle medesime Autorità, in base all'art. 57, possono essere distinti[148] in poteri di:

- indagine: finalizzati a sottoporre a verifica l'osservanza del Regolamento come le possibili violazioni. In questo ambito si colloca il potere di ingiungere al Titolare o al Responsabile del trattamento di fornire determinate informazioni; di effettuare il riesame delle certificazioni; di notificare al Titolare o al Responsabile del trattamento le presunte violazioni del GDPR;

- correttivi: rivolgere avvertimenti al Titolare o Responsabile del trattamento in merito a presunte violazioni del GDPR; ingiungere al Titolare del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti derivanti dal Regolamento; di conformare i trattamenti alle relative disposizioni; di comunicazione agli interessati una violazione di dati personali; può ordinare la rettifica o la cancellazione di dati personali; revocare la certificazione oppure ingiungere all'organismo di certificazione di ritirare la certificazione oppure di non rilasciarla se i requisiti non sono soddisfatti; infliggere una sanzione amministrativa pecuniaria;

- autorizzativi e consultivi, nei confronti dei diversi soggetti coinvolti nel trattamento dei dati, tra cui il potere di consulenza preventiva che può fornire al titolare del trattamento (articolo 36 del GDPR); il potere di rilascio di pareri sui codici di condotta e le certificazioni (approvando anche i criteri per i meccanismi di certificazioni); il potere di autorizzazione degli accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti azionabili per gli interessati; il potere di autorizzare le clausole contrattuali e le altre disposizioni di cui all'art. 46, paragrafo 3; il potere di approvare norme vincolanti di impresa (art. 47).

nel suo territorio o il trattamento effettuato da un titolare del trattamento o da un responsabile del trattamento non stabilito nell'Unione europea riguardante interessati non residenti nel suo territorio. Ciò dovrebbe includere l'esame dei reclami proposti dall'interessato, lo svolgimento di indagini sull'applicazione del regolamento e la promozione della sensibilizzazione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali.»

[147]Su tale distinzione e sul contenuto di ciascuna funzione, cfr. F. FRENI, *Le* Authorities, in *Adempimenti privacy per professionisti e aziende*, cit., 167.

[148] Per questa distinzione, ancora, cfr. F. FRENI, *Le* Authorities, in *Adempimenti privacy per professionisti e aziende*, cit., 174.