Il nuovo Regolamento generale sulla protezione dei dati: alcune considerazioni informatico-giuridiche

www.dimt.it/2016/05/31/il-nuovo-regolamento-generale-sulla-protezione-dei-dati-alcune-considerazioni-informatico-giuridiche/

di **Silvia Martinelli**

Abstract

Il 4 maggio 2016 è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il Regolamento europeo n. 679/2016 in materia di protezione dei dati personali. L'articolo, previa una panoramica sugli obiettivi della riforma e sul lungo procedimento che ha portato all'approvazione, analizza alcuni degli elementi di novità introdotti dal Regolamento nella disciplina della protezione dei dati personali delle persone fisiche, anche raffrontando quanto ivi previsto con le disposizioni di cui alla Direttiva 95/46/CE, nonché con la disciplina nazionale.

Una particolare attenzione è dedicata all'ambito di applicazione del Regolamento e alla nuova formulazione dei diritti dell'interessato. Sono trattati, in particolare, il diritto di accesso, il diritto alla portabilità dei dati, il diritto di rettifica, il diritto alla cancellazione del trattamento ("diritto all'oblio"), il diritto di limitazione del trattamento e il diritto di opposizione. Sono, inoltre, introdotti i concetti di "privacy by design" e "privacy by default", i principi applicabili alla valutazione d'impatto, il Data Protection Officer, l'obbligo di notificazione dei data breach e il nuovo trattamento sanzionatorio.

On May 4, 2016 the Regulation n. n. 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (EU General Data Protection Regulation, also known as "GDPR"), was published in the Official Journal of the European Union. The article, after an overview of the aims of the reform and the long legislative approval process, examines some of the new elements introduced by the Regulation on the protection of personal data of individuals, even comparing new provisions with the provisions laid down in the Directive 95/46/CE as well as with Italian legislation.

The essay focuses on the material and territorial scope and on the rights of the data subject. Specially, it describes the right of access, the right to data portability, the right to rectification, the right to erasure ("right to be forgotten"), the right to restriction of processing and the right to object. Afterwards it introduces the concepts of "privacy by design" and "privacy by default", the principles applicable to the impact assessment, the Data Protection Officer, the notification of data breaches and the new sanctioning treatment.

Sommario

1. Gli obiettivi della riforma della normativa sulla protezione dei dati e il lungo procedimento che ha portato alla sua approvazione

Le nuove tecnologie e la rapidità della loro evoluzione hanno trasformato l'economia e le relazioni sociali amplificando la circolazione dei dati personali e ponendo sempre nuove sfide per la loro protezione.

L'Unione europea, da tempo, riconosce il diritto alla protezione dei dati personali quale diritto fondamentale, sancito dall'articolo 8 della Carta dei diritti fondamentali dell'Unione europea [1], nonché dall'art. 16, primo paragrafo del TFUE, introdotto dal trattato di Lisbona [2], ai sensi dei quali «ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano».

La protezione dei dati personali è tutelata dal diritto dell'Unione mediante diversi strumenti, tra i quali figura in primo luogo la direttiva 95/46/CE del Paramento europeo e del Consiglio del 24 ottobre 1995, pietra angolare nell'impianto della vigente normativa europea in materia di protezione dei dati, relativa «alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati» [3].

Sin dalla lettura della rubrica appare evidente il duplice fine che muove il legislatore europeo: la tutela del diritto delle persone alla tutela dei dati che le riguardano, considerato diritto fondamentale dell'individuo, e la libera circolazione dei dati, divenuta ormai essenziale in un mondo globalizzato e interconnesso per consentire la realizzazione di un mercato unico europeo.

Dalle quattro libertà fondamentali, simbolo dell'integrazione comunitaria, che hanno portato alla realizzazione del mercato interno (libera circolazione delle persone, libera circolazione delle merci, libera circolazione dei servizi e libera circolazione dei capitali), muove la libertà di circolazione del dato, essenziale e ineludibile nell'odierna società iperconnessa per l'affermazione delle quattro libertà e la realizzazione del mercato unico europeo.

La Direttiva è stata ritenuta insufficiente al raggiungimento di tali scopi, in quanto inidonea a stabilire un uniforme applicazione del diritto alla protezione dei dati personali. Lo strumento della direttiva, infatti, una volta emanata dalle istituzioni europee, richiede un recepimento da parte dei legislatori nazionali dei singoli Stati membri, i quali devono rispettare quanto nella direttiva stessa previsto richiamandolo nelle loro legislazioni, con un certo margine di discrezionalità con riguardo alla specificazione del suo contenuto, imponendo la direttiva soltanto un obbligo di risultato.

A ciò si aggiunga che l'interpretazione ai fini dell'applicazione delle normative nazionali in materia di protezione dei dati personali è affidata, oltre che ai legislatori ed alle Corti, alle Autorità Garanti. Ciò ha portato alla presenza, nei singoli Stati membri, di differenti linee interpretative e diversi orientamenti in sede di applicazione che, seppur concernenti singoli e limitati aspetti della protezione del dato, hanno condotto ad una applicazione non uniforme e alla compresenza di livelli di protezione diversi. A questi margini di discrezionalità esercitati dagli Stati membri, si aggiungono gli ambiti nei quali la Direttiva non interviene, nei quali i singoli Stati hanno legiferato secondo il proprio intendimento.

Il nuovo Regolamento si pone come obiettivo, in primo luogo, la riduzione della frammentazione nell'applicazione della normativa in materia di protezione dei dati personali nei singoli Stati membri e l'affermazione di un'applicazione che elimini tali disparità, che sia coerente, omogenea, e idonea a consentire una tutela equivalente in tutti gli Stati membri, al fine di rafforzare il mercato unico e rimuovere gli ostacoli che ne limitano la piena realizzazione, nonché lo sviluppo dell'economia digitale in tutto il mercato interno ovvero il cosiddetto mercato unico digitale [4].

Lo strumento legislativo del regolamento è, infatti, applicabile direttamente in tutti gli Stati membri dal momento della sua entrata in vigore, senza la necessità di un recepimento da parte dei Legislatori nazionali, eliminandosi così l'operazione nella realizzazione della quale gli Stati membri introducono delle differenziazioni e precisazioni rispetto a quanto nella direttiva previsto.

Inoltre, il nuovo Regolamento intende rafforzare e disciplinare in modo più dettagliato e coerente i diritti degli interessati e gli obblighi di coloro che effettuano il trattamento dei dati, nonché i poteri dei soggetti che assicurano il rispetto delle norme e applicano le sanzioni e, al contempo, razionalizzare la normativa esistente e gli orientamenti

dei Garanti europei, stratificatisi alla luce delle precisazioni e specificazioni rese necessarie dall'introduzione e dall'utilizzo sempre più massivo da parte degli operatori economici di nuove tecnologie.

Vi è nella riforma anche la volontà di garantire un maggior rispetto della privacy degli individui e una maggior efficacia delle norme, aumentando l'aderenza delle condotte a quanto nel Regolamento stesso prescritto.

Infine, la riforma vuole intervenire nella diffusa percezione di rischio che le persone hanno nell'effettuare operazioni online, aumentando la loro protezione e fiducia mediante una più diffusa e percepita certezza giuridica.

Sebbene siano trascorsi anni dalla prima proclamazione di tali intenti e obiettivi, l'elaborazione e la definitiva approvazione del Regolamento ha richiesto un lungo e lento processo di elaborazione, consultazione e condivisione e, solo nell'aprile del 2016, la riforma della normativa europea a tutela dei dati personali è giunta, finalmente, a conclusione.

Il nuovo Regolamento «relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)», pubblicato in Gazzetta Ufficiale dell'Unione europea il 4 maggio 2016, è stato approvato dal Parlamento europeo in sessione plenaria il 14 aprile 2016, concludendo in tal modo un procedimento legislativo che ha dovuto attendere anni prima di poter veder la luce nella sua versione definitiva.

Sin dal 2009, infatti, la Commissione aveva avviato pubbliche consultazioni e dialoghi con le parti interessate, al fine di avviare un processo di riforma in materia [5]. Nel 2010 è stata pubblicata la Comunicazione della Commissione «Un approccio globale alla protezione dei dati personali nell'Unione europea» [6] nella quale venivano esposti i principali obiettivi della riforma: l'armonizzazione della normativa in materia al fine di rimuovere gli ostacoli e le difficoltà incontrate dagli imprenditori, una maggiore chiarezza e certezza giuridica e una più diffusa e completa consapevolezza da parte dei cittadini europei dell'importanza dei dati a loro riferiti o riferibili e della loro tutela.

Nel corso del 2011, dal confronto tra l'Autorità garante europea e le Autorità garanti nazionali con la Commissione, l'esigenza di un quadro normativo solido, coerente e trasversale che rafforzasse i diritti delle persone fisiche e al contempo consolidasse il mercato interno si è delineata e concretizzata nella previsione dell'elaborazione e approvazione di un regolamento europeo in sostituzione della Direttiva 95/46/CE e una direttiva volta a sostituire la Decisione quadro 2008/977/GAI16, relativa alla protezione dei dati personali trattati ai fini di prevenzione, indagine, accertamento o perseguimento dei reati e relative attività giudiziarie.

Ottenuto un primo parere favorevole da parte del Parlamento e del Consiglio nel 2011, la prima proposta di regolamento del Parlamento europeo e del Consiglio «concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)» [7] è presentata dalla Commissione il 25 gennaio 2012.

Tuttavia, solo dopo quasi tre anni di trattative, nel dicembre 2015, il Parlamento europeo e il Consiglio, rispettivamente a livello di commissione e ambasciatori, hanno raggiunto un accordo sul testo delle nuove norme in materia di protezione dei dati [8].

In data 8 aprile 2016 il testo del Regolamento è stato approvato dal Consiglio e il 14 aprile 2016 il Parlamento europeo lo ha approvato in sessione plenaria, completando così il lungo iter legislativo.

Il Regolamento così approvato riprende, in larga parte, quanto già previsto dalla Direttiva, mantenendo una concezione della privacy basata sul consenso e sul rispetto di alcuni principi fondamentali (liceità, proporzionalità, correttezza, trasparenza, minimizzazione dei dati, etc.) e conserva l'affidamento ai legislatori nazionali di ampi margini di discrezionalità.

L'intervento modificativo si incentra sul rafforzamento dei diritti dell'interessato, mediante una loro più precisa e ampia specificazione, e sulla responsabilizzazione degli operatori, sui quali, invertendosi l'onere della prova, ricade

ora il compito di aver attuato misure adeguate alla gestione dei rischi che il trattamento di dati effettuato comporta.

Nei due anni che decorrono dalla pubblicazione del Regolamento in Gazzetta Ufficiale sino alla sua entrata in vigore, prevista per maggio 2018, saranno necessari interventi interpretativi e di coordinamento con le norme preesistenti, ad opera sia delle istituzioni europee, sia dei legislatori e delle Autorità garanti nazionali.

2. L'ambito di applicazione del Regolamento e le definizioni in esso fornite

Per comprendere la portata del Regolamento generale sulla protezione dei dati occorre guardare, in prima analisi, al suo ambito di applicazione, al quale è dedicato il Primo Capo del Regolamento.

Una prima delimitazione è fornita dall'art. 2, ai sensi del quale 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» [9].

Si può osservare, quindi, in primo luogo, che il Regolamento è applicabile sia al trattamento effettuato in ambito digitale che al trattamento effettuato mediante mezzi analogici. Tuttavia, esso non si applica a tutte le tipologie di trattamento e sono posti limiti all'ambito di applicazione territoriale, sebbene grazie alla definizione dell'ambito di applicazione nel Regolamento formulata, forte sia la forza espansiva anche al di fuori del territorio dell'Unione.

L'art. 3 del Regolamento, che concerne l'applicazione in ambito territoriale, prevede tre ipotesi nelle quali 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 nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione»;

- «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:

1. a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
2. b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione»;

- «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».

Il Regolamento è, quindi, applicabile sia ai trattamenti di dati personali effettuati da titolari del trattamento (o responsabili) stabiliti nel territorio dell'Unione, sia ai trattamenti che, sebbene effettuati da titolari stabiliti in territorio extra-europeo, concernono soggetti che "si trovano" nel territorio dell'Unione, in quanto volti a fornire a tali soggetti beni o servizi o a monitorare i loro comportamenti.

Con riguardo ai trattamenti effettuati da titolari (o responsabili) stabiliti nel territorio dell'Unione, di cui al primo punto sopraelencato, soggiunge a chiarimento il considerando n. 22, il quale precisa quanto segue:

«Qualsiasi trattamento di dati personali effettuato nell'ambito delle attività di uno stabilimento di un titolare del trattamento o responsabile del trattamento nel territorio dell'Unione dovrebbe essere conforme al presente regolamento, indipendentemente dal fatto che il trattamento avvenga all'interno dell'Unione».

Fondamentale ai fini della comprensione della reale portata applicativa di tale disposizione è la definizione di stabilimento, con riguardo alla quale il medesimo considerando n. 22 precisa: «lo stabilimento implica l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile […] non è determinante la forma giuridica

assunta, sia essa una succursale o una filiale dotata di personalità giuridica».

La nozione di stabilimento non è, dunque, vincolata a particolari requisiti formali ma è, anzi, connessa al luogo di effettivo e reale svolgimento dell'attività, essendo sufficiente la sussistenza di una stabile organizzazione.

Di più complessa interpretazione è la seconda categoria sopraelencata, che prevede l'applicazione del Regolamento quando le attività di trattamento riguardano l'offerta di beni o servizi a soggetti che si trovano nell'Unione o il monitoraggio di loro comportamenti che hanno luogo nel territorio dell'Unione.

Il considerando n. 23, sul punto, specifica che per determinare se vi sia un'offerta di beni o servizi occorre verificare in concreto se il titolare del trattamento abbia intenzione di vendere beni o servizi nell'Unione ed è irrilevante a tal fine l'esistenza o meno di un pagamento.

Per le attività svolte online, viene, inoltre, precisato che la mera accessibilità del sito web, di un indirizzo di posta elettronica, di altre coordinate di contatto o l'impiego di una lingua abitualmente utilizzata sono insufficienti per accertare tale intenzione. Tuttavia, fattori quali l'utilizzo della lingua o della moneta abitualmente utilizzata in uno Stato membro, la possibilità di ordinare i beni o servizi nella lingua di uno Stato membro, la menzione di clienti o utenti che si trovano nell'Unione, possono evidenziare l'intenzione di offrire beni o servizi agli interessati nell'Unione.

Nonostante tali precisazioni, in ordine alla sussistenza di tale requisito, solo la sua applicazione ad opera della giurisprudenza, mediante verifica in concreto, potrà fornire maggiori certezze.

Con riguardo alla rilevazione del monitoraggio, i problemi interpretativi sono, forse, maggiori. Il considerando n. 24 specifica che per stabilire se vi sia un monitoraggio occorre verificare se le persone siano tracciate su internet e profilate e se le informazioni sono utilizzate per adottare decisioni che riguardano i soggetti cui le informazioni si riferiscono; ma anche a seguito di tale precisazione, permangono dubbi in merito alla determinazione delle condotte che possano costituire "monitoraggio" e, anche per quanto concerne il "tracciare" le persone su internet, non è chiaro se ogni tipologia di "traccia" lasciata dagli utenti durante la navigazione online possa essere considerata monitoraggio. Ulteriori problemi si rinvengono nella difficoltà di determinare, con riguardo alle attività online, il luogo nel quale i comportamenti monitorati avvengono.

Per quanto concerne, invece, le particolari tipologie di trattamento escluse dall'ambito di applicazione, alle quali si accennava in precedenza, rilevano, in primo luogo, i dati relativi a persone decedute e i dati trattati in forma anonima e che non consentono l'identificazione del soggetto interessato, alle quali il Regolamento non si applica in quanto non rientranti nella definizione di dato personale fornita dallo stesso regolamento, la quale considera dato personale solamente il dato che consenta l'identificazione della persona a cui si riferisce.

Svolta questa prima precisazione, rileva l'elenco di cui al secondo comma dell'art. 2, che prevede l'esclusione dei seguenti trattamenti:

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

1. b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE [10];
2. c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;
3. d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati, esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse».

Con riguardo alle lettere c e d alcune precisazioni si rendono necessarie. In particolare, la lettera c, è precisata dal considerando n. 18, che prevede che il Regolamento non si applichi al trattamento effettuato da persone fisiche nell'ambito di attività a carattere esclusivamente personale o domestico, in assenza di una connessione con

un’attività commerciale o professionale. Al medesimo considerando, sono, inoltre, elencate alcune esemplificazioni che potrebbero essere ricomprese in tale definizione, quali la corrispondenza e gli indirizzari o l’uso dei social network.

Per quanto concerne, invece, la lettera d, da leggersi in combinato disposto con il considerando n. 19 [11], essa esclude dall’ambito di applicazione del Regolamento i trattamenti effettuati ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché ai fini di salvaguardia e prevenzione delle minacce alla pubblica sicurezza, in quanto rientranti nell’ambito di applicazione della Direttiva che sostituirà la Decisione quadro 2008/977/GAI16.

Inoltre, in tale materia permane una più ampia autonomia in capo ai Legislatori nazionali, che possono mantenere o introdurre disposizioni più specifiche, nonché adottare disposizioni legislative volte a limitare obblighi e diritti, purché la limitazione costituisca una misura necessaria e proporzionata in una società democratica a tutela della pubblica sicurezza, per l’accertamento e il perseguimento di reati, per l’esecuzione delle sanzioni penali e per la prevenzione di minacce alla sicurezza pubblica (considerando n. 20) [12].

Con riguardo ai trattamenti effettuati dalle autorità giurisdizionali e giudiziarie, inoltre, ai fini della tutela dell’indipendenza e autonomia del potere giurisdizionale, vi sono peculiarità anche in relazione al controllo del rispetto della normativa in materia di protezione dei dati personali, che deve essere affidato a organismi specifici all’interno del medesimo sistema giudiziario.

Sono esclusi dall’ambito di applicazione anche i trattamenti effettuati dalle Pubbliche Amministrazioni — quali le autorità fiscali e doganali, di indagine finanziari, le autorità amministrative indipendenti e le autorità di vigilanza nel settore finanziario — ai fini di specifiche indagini nell’interesse generale.

È, infine, fatta salva la disciplina di cui alla Direttiva 2000/31/CE, cosiddetta direttiva in materia di commercio elettronico, che rimane impregiudicata dall’adozione del Regolamento, anche con riguardo alla disciplina in essa prevista agli articoli 12, 13 e 14 e che disciplinano la responsabilità degli intermediari di servizi [13].

Anche ai fini della comprensione dell’ambito al quale il Regolamento si applica, è necessario analizzare e valutare le definizioni che in esso sono fornite e, in primo luogo, la stessa definizione di dato personale.

Ai sensi dell’articolo 4, primo comma, del Regolamento per “dato personale” s’intende «qualsiasi informazione riguardante una persona fisica identificata o identificabile» e la persona a cui i dati si riferiscono è definita come “interessato”. Per “identificabile”, «la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all’ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale» [14].

Tale concetto, definito in modo molto ampio e ricomprendente ogni tipologia di dato che sia riferibile a una persona fisica, è, inoltre, approfondito al considerando n. 26, il quale specifica che la “pseudonimizzazione” dei dati non è sufficiente affinché la persona interessata non sia identificabile, in quanto i dati potrebbero essere attribuiti ad essa mediante l’utilizzo di ulteriori informazioni, ma occorre effettuare una valutazione in concreto che consideri i mezzi che potrebbero essere utilizzati ai fini dell’identificazione e, in particolare, «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».

La pseudonimizzazione consente, quindi, di considerare i dati come trattati in forma anonima e, pertanto, esclusi dall’applicazione del regolamento, solo ove siano in concreto «resi sufficientemente anonimi da impedire o da non consentire più l’identificazione dell’interessato».

Con riguardo al “trattamento”, il Regolamento fornisce un’ampia definizione che ricalca, seppur con qualche modificazione, quella già in precedenza presente dalla Direttiva: «qualsiasi operazione o insieme di operazioni,

compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione» [15].

Tale definizione è idonea a ricomprendere sia i trattamenti effettuati mediante elaborate elettronico, che i trattamenti analogici. Inoltre, l'ampia elencazione delle attività svolte sui dati personali, consente di ricomprendere quasi ogni tipologia di attività che comporti il loro utilizzo.

Nel Regolamento compaiono anche definizioni "nuove", che non erano presenti nel testo della Direttiva, tra le quali la "profilazione", definita come «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»; la "pseudonimizzazione", ovvero «il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile»; non presenti nel testo della Direttiva [16].

Tali definizioni specificano alcuni concetti che erano stati oggetto dell'attività normativa, regolativa e giurisprudenziale degli Stati membri e, in particolare, per quanto riguarda il nostro Paese, era già divenuta oggetto d'interpretazione da parte del Garante privacy.

Con riguardo alle definizioni di titolare e responsabile del trattamento, sebbene la Direttiva li definisse in modo analogo, il Legislatore italiano in sede di recepimento e, successivamente, anche con l'emanazione del d.lgs. 196/2003 ha, da sempre, utilizzato una terminologia diversa rispetto a quella utilizzata dal Legislatore europeo. In particolare, ai sensi del Codice Privacy "responsabile" è «la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali", mentre "incaricati" sono "le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile».

In merito a tale divergenza definitoria il Garante italiano si è espresso sin dal 13 aprile 2016, dichiarando che «i termini "Titolare del trattamento" e "Responsabile del trattamento", già presenti nel Codice Privacy italiano, compariranno anche nei testi italiani del Regolamento europeo in materia di protezione dei dati personali e della Direttiva che regola i settori di prevenzione, contrasto e repressione dei crimini, entrambi in via di approvazione definitiva a Bruxelles», al fine di evitare «un inutile sforzo adattativo e interpretativo» [17].

3. Principi, obblighi di trasparenza, diritto di accesso e portabilità dei dati

Come anticipato in precedenza, l'impianto della Direttiva 95/46/CE è stato mantenuto e, con esso, i principi fondamentali applicabili al trattamento, cui è dedicato il Capo II del Regolamento. Pertanto, così come già in precedenza, i dati personali devono essere:

1. a) trattati «in modo lecito, corretto e trasparente nei confronti dell'interessato» [18] (principi di liceità, correttezza e trasparenza);
2. b) per «finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità» [19] (limitazione della finalità);
3. c) «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati» [20] (minimizzazione dei dati);
4. d) «esatti e, se necessario, aggiornati» [21] (esattezza);

5. e) «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» [22] (limitazione della conservazione);
6. f) «trattati in maniera da garantire un'adeguata sicurezza dei dati personali» [23] (sicurezza, integrità e riservatezza).

Con riguardo al principio di liceità del trattamento, il trattamento è lecito se l'interessato ha espresso il suo consenso al trattamento o se esso è necessario per l'esecuzione di un contratto, l'adempimento di un obbligo legale, la salvaguardia di interessi vitali per una persona fisica, l'esecuzione da parte del titolare di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, il perseguimento di un legittimo interesse ove non prevalgano i diritti e le libertà del soggetto interessato [24].

Il consenso, ove necessario, deve essere libero, informato e fornito per iscritto, «in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro» e il titolare del trattamento deve essere in grado di dimostrare che l'interessato l'ha prestato [25]. L'interessato ha, inoltre, diritto di revocarlo, in qualsiasi momento, e di tale diritto di revoca deve essere informato [26].

Il principio di trasparenza, di cui all'art. 5, primo comma, lett. a) del Regolamento, è, forse, il principio che maggiormente è divenuto oggetto dell'intervento modificativo operato dal Legislatore europeo, volto a rafforzarne la portata. La Prima Sezione del Capo III del Regolamento è, infatti, integralmente dedicata a tale principio.

Le informazioni che il titolare del trattamento deve fornire all'interessato, devono sempre essere rese «in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro» [27] e, qualora l'interessato effettui una richiesta ai sensi degli articoli da 15 a 20 (diritto di accesso, rettifica, cancellazione, limitazione del trattamento, portabilità dei dati), le informazioni oggetto della richiesta devono essere rese senza ritardo e, al più tardi, entro un mese dal ricevimento della richiesta stessa [28].

I diritti di cui agli artt. da 15 a 20 devono poter sempre essere esercitati in modo gratuito e il titolare del trattamento può ottemperare o meno la richiesta [29]. Qualora egli decida di non ottemperare alla richiesta deve, comunque, entro un mese, comunicare all'interessato il diniego e la sua motivazione, nonché informarlo della possibilità di proporre reclamo innanzi alle autorità di controllo o innanzi alle autorità giudiziarie.

Il titolare deve, inoltre, fornire all'interessato una lunga serie di informazioni, elencate agli artt. 13 e 14 del Regolamento. L'art. 13 del Regolamento elenca le informazioni che il titolare deve fornire all'interessato qualora i dati personali siano raccolti presso di lui [30], da fornire anche in caso di modifica delle finalità di un trattamento già in essere, e l'art. 14 elenca quelle da rendersi ove i dati non siano ottenuti presso l'interessato [31]. In quest'ultimo caso, le informazioni devono essere rese entro un tempo ragionevole dall'ottenimento dei dati personali e, al più tardi, entro un mese [32].

Sono comunque esclusi, dall'applicazioni di tali obblighi informativi [33], i trattamenti per i quali: l'interessato disponga già delle informazioni, la loro comunicazione risulti impossibile o richieda uno sforzo sproporzionato [34]; l'ottenimento o la comunicazione sono «espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato»; i dati personali debbano rimanere riservati [35].

Oltre alla previsione degli obblighi informativi, all'interessato è attribuito un diritto di accesso, regolato dall'art. 15 del Regolamento, che consiste nel diritto dell'interessato di sapere se è o meno in corso un trattamento di dati personali che lo riguardano e, qualora sia in corso un trattamento, il diritto ad ottenere le informazioni ad esso relative.

In particolare, le informazioni che devono essere fornite sono: «a) le finalità del trattamento; b) le categorie di dati personali in questione; c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali; d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale

periodo; e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento; f) il diritto di proporre reclamo a un'autorità di controllo; g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine; h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato» [36].

Si tratta di un'elencazione molto ampia e dettagliata se confrontata con quanto in precedenza previsto dalla Direttiva 95/46/CE, accompagnata da nuove precisazioni con riguardo alle modalità e ai costi per l'esercizio del diritto, in precedenza appena accennate.

Con riguardo ai costi, si applica il principio della gratuità, salvo per il caso in cui l'interessato richieda più copie, nel qual caso il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi.

Per quanto concerne le modalità tramite le quali le informazioni devono essere fornite, il Regolamento prevede che il titolare del trattamento predisponga i mezzi per inoltrare le richieste per via elettronica, in particolare ove i dati personali siano trattati con mezzi elettronici.

Inoltre, qualora l'interessato presenti la richiesta mediante mezzi elettronici, le informazioni devono essere fornite in un formato elettronico "di uso comune", salvo che vi sia un'indicazione diversa da parte dello stesso interessato.

Al fine di evitare che soggetti terzi possano venire illegittimamente a conoscenza dei dati trattati, al titolare spetta, anche, il compito di verificare l'identità dell'interessato che richieda l'accesso, adottando tutte le misure ragionevoli.

Con riguardo, infine, ai tempi per l'evasione delle richieste, il titolare del trattamento è tenuto a rispondere senza ingiustificato ritardo, al più tardi entro un mese.

L'interessato ha, inoltre, diritto di ricevere dal titolare copia dei dati personali oggetto del trattamento, cosiddetto "diritto alla portabilità dei dati", di nuova introduzione, che ove esperito consente all'interessato 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 e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti».

Esso può essere esercitato qualora: «a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e b) il trattamento sia effettuato con mezzi automatizzati» [37].

Sul punto, il considerando n. 68, precisa che il diritto alla portabilità dei dati «dovrebbe applicarsi qualora l'interessato abbia fornito i dati personali sulla base del proprio consenso o se il trattamento è necessario per l'esecuzione di un contratto», mentre «non dovrebbe applicarsi qualora il trattamento si basi su un fondamento giuridico diverso dal consenso o contratto».

Il diritto alla portabilità dei dati non si applica, però, in caso di 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 e, più precisamente, come specificato dal considerando n. 68, non dovrebbe essere esercitato per i trattamenti effettuati nell'esercizio di funzioni pubbliche o pubblici poteri o per l'esecuzione di un compito svolto nel pubblico interesse e quando il trattamento è necessario per l'adempimento di un obbligo legale. Inoltre, il suo esercizio non deve ledere i diritti e le libertà altrui.

L'interessato può, infine, richiedere, anche, la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, ove ciò sia tecnicamente fattibile.

I formati da utilizzarsi per la trasmissione, sono specificati al considerando n. 68, nel quale è incoraggiato l'utilizzo di

formati interoperabili, sebbene non vi sia un obbligo in capo ai titolari di adottare o mantenere sistemi di trattamento tecnicamente compatibili [38].

4. La nuova disciplina dei dati sensibili e la profilazione

Vi sono alcune categorie di dati e alcune tipologie di trattamento che comportano una maggiore invasione della sfera personale della persona.

L'articolo 9 del Regolamento, dedicato al «trattamento di categorie particolari di dati personali», prevede il divieto di trattare alcune tipologie di dati personali, ovvero quelle che rivelino «l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona».

Il trattamento di tali dati, ove il divieto di trattamento è la regola generale, è tuttavia, consentito se:

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

1. b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
2. c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
3. d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;
4. e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
5. f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
6. g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
7. h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;
8. i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

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

Analoga previsione, sebbene meno dettagliata, era già prevista all'art. 8 della Direttiva 95/46/CE [39]. Di essa, però, il Legislatore italiano, in sede di recepimento, aveva dato una sua particolare interpretazione, elaborando la cosiddetta categoria dei dati sensibili.

Il Codice Privacy italiano attualmente in vigore prevede, infatti, particolari modalità per il trattamento di alcune tipologie di dati denominate "dati sensibili" e definiti «i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale» [40].

Per essi, il Codice prevede una disciplina del tutto peculiare, idonea ad offrire agli interessati maggiori garanzie. Ai sensi dell'art. 26 del Codice, infatti, per poter effettuare il trattamento è necessario il consenso della persona interessata e la previa autorizzazione del Garante [41], salvo che si tratti di trattamento effettuato da soggetti pubblici — consentito se autorizzato da espressa disposizione di legge, che precisi le tipologie di dati che possono essere trattati e le finalità, o vi sia espressa autorizzazione del Garante — o si tratti delle particolari tipologie di trattamento elencate ai commi terzo e quarto dell'art. 26 del Codice.

Dubbio è se il Legislatore italiano voglia mantenere tale particolare categoria di dati personali anche a seguito dell'entrata in vigore del Regolamento, sebbene il quarto comma dell'art. 9 del Regolamento sembrerebbe lasciare margine di discrezionalità ai legislatori nazionali, prevedendo: «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».

In tal senso, si esprime anche il considerando n. 10 del Regolamento, nel quale è affermato che il Regolamento stesso prevede per gli Stati membri un margine di manovra per precisarne le norme, consentendo la previsione di condizioni più restrittive per «specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito", e ciò "anche con riguardo al trattamento di categorie particolari di dati personali ("dati sensibili")».

I dati sensibili, ovvero quelle particolari categorie di dati maggiormente idonee ad invadere la sfera più personale dell'interessato, nonché più facilmente utilizzabili in modo discriminatorio, continueranno, quindi, a godere di tutela più ampia rispetto alle categorie di dati che coinvolgono aspetti più superficiali e meno riservati della vita degli individui. Spetterà, tuttavia, al Legislatore nazionale decidere se mantenere quanto già previsto dal Codice Privacy, con le opportune revisioni o modificazioni o se adottare una normativa meno dettagliata e più vicina a quanto nel Regolamento stesso stabilito.

Un altro trattamento particolarmente invasivo della sfera privata dell'individuo è quello operato ai fini della profilazione. Il Regolamento, a differenza della Direttiva, prevede tale pratica espressamente, definendola quale «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» ed è soggetta alle norme che disciplinano il trattamento dei dati personali [42].

In particolare, ai sensi del Regolamento, l'interessato dovrebbe essere informato dell'esistenza di una profilazione, delle finalità e delle sue conseguenze [43] e i dati tramite attività elaborati dovrebbero poter essere utilizzati per "prendere decisioni" solo qualora tale possibilità sia specificamente prevista «dal diritto dell'Unione o degli Stati

membri cui è soggetto il titolare del trattamento, anche a fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale secondo i regolamenti, le norme e le raccomandazioni delle istituzioni dell'Unione o degli organismi nazionali di vigilanza e a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento, o se è necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, o se l'interessato ha espresso il proprio consenso esplicito» [44].

Non solo, anche nei casi sopradescritti permane un obbligo di apprestare garanzie adeguate a garantire il rispetto dei diritti dell'interessato concernenti «la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione» [45]. Ad esse devono, inoltre, accompagnarsi misure tecniche e organizzative adeguate «al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti» [46].

In materia di profilazione, sebbene nulla fosse esplicitamente previsto nella Direttiva 95/46/CE, il Garante privacy italiano ha, progressivamente, emanato numerosi atti provvedimenti e chiarimenti, di cui da ultimo le dettagliate «Linee guida in materia di trattamento di dati personali per profilazione on line», del 19 marzo 2015 [47].

Tale materia è, inoltre, in parte trattata dalla Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002, «relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)», che disciplina, tra l'altro la conservazione e l'utilizzazione dei dati relativi al traffico telematico e all'ubicazione degli utenti, la cui disciplina è stata recepita in Italia all'interno del Codice Privacy [48], e successivamente modificata a seguito degli interventi del Legislatore europeo sulla stessa Direttiva [49].

Nel corso dei prossimi due anni diverrà più chiaro come debbano coordinarsi la disciplina del Regolamento e quella prevista dalla Direttiva 2002/58/CE, e si avrà modo di conoscere gli intendimenti del Legislatore e del Garante italiano sul mantenimento delle linee e dei principi già adottati e applicati nel corso degli anni.

5. Il diritto di rettifica, il diritto alla cancellazione ("diritto all'oblio"), il diritto di limitazione del trattamento e il diritto di opposizione

Tra i diritti attribuiti al soggetto interessato, oltre al diritto di accesso di cui si è detto in precedenza, vi sono il diritto di rettifica, il diritto alla cancellazione ("diritto all'oblio"), il diritto di limitazione del trattamento e il diritto di opposizione.

Il diritto di rettifica, affermato dall'art. 16 del Regolamento, è il diritto dell'interessato «di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo» e il diritto alla cancellazione, sancito dall'art. 17, è il diritto dell'interessato «di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo».

Ai fini della loro attuazione gli operatori devono «prevedere modalità volte ad agevolare l'esercizio, da parte dell'interessato» [50], consentendo l'inoltro delle richieste per via elettronica [51], e senza costi a carico del richiedente.

Al diritto alla cancellazione sono, tuttavia, posti alcuni limiti. Esso può essere attuato, in primo luogo, in due casi: se il trattamento sia effettuato subordinatamente alla prestazione del consenso, la revoca dello stesso costituisce requisito necessario e sufficiente ai fini della cancellazione; ove, invece, i dati personali siano stati raccolti per finalità o tipologie di trattamento per le quali il consenso non è richiesto, la cancellazione potrà essere attuata ove i

dati personali non siano più necessari rispetto alle finalità per le quali sono stati raccolti o trattati.

Ad essi si aggiungono i casi nei quali: l'interessato si opponga al trattamento e non sussistano motivi legittimi prevalenti per procedere al trattamento; i dati personali siano stati trattati illecitamente; la cancellazione sia necessaria per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; i dati personali siano stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1, per i quali è previsto un tempo di conservazione determinato.

In capo al titolare del trattamento, ove sia richiesta una cancellazione dei dati e sussistano i predetti requisiti, è posto un obbligo non solo di cancellazione presso i suoi archivi, ma, ove gli abbia resi pubblici, anche un obbligo di comunicazione ai soggetti terzi e titolari di differente trattamento dei medesimi dati, che stanno trattando dati personali di cui l'interessato ha richiesto la cancellazione, ricomprendente «qualsiasi link, copia o riproduzione dei suoi dati personali". Tale obbligo di comunicazione deve essere attuato "tenendo conto della tecnologia disponibile e dei costi di attuazione» [52].

Altri interessi possono, tuttavia, essere ritenuti prevalenti sul diritto alla cancellazione, che dovrebbe essere, quindi, negato qualora la conservazione 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» [53].

Spetta, inoltre, all'interessato il cosiddetto "diritto di limitazione del trattamento", previsto all'art. 18 ed esercitabile nei casi nei quali: l'interessato contesti l'esattezza dei dati personali, «per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali»; il trattamento sia illecito e l'interessato si opponga alla cancellazione dei dati personali, chiedendo invece la limitazione del loro utilizzo; il titolare del trattamento non ne abbia più bisogno, ma essi siano «necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria»; in caso di opposizione al trattamento ed attesa della «verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato».

In tutti i casi di esercizio di uno dei diritti sopradescritti (diritto alla cancellazione, diritto di rettifica, diritto alla limitazione del trattamento), il titolare è tenuto a comunicare «a ciascuno dei destinatari cui sono stati trasmessi i dati personali» le rettifiche, cancellazioni o limitazione del trattamento.

Infine, fondamentale diritto dell'interessato, presente ed ampiamente articolato sin dalla Direttiva 95/46/CE, è il diritto di opposizione, che consente all'interessato di opporsi «in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano» [54].

A seguito dell'esercizio di tale diritto il titolare può continuare a trattare i dati solo ove «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» [55].

6. La "privacy by design" e privacy "by default", la valutazione d'impatto, il Data Protection Officer, i data breach e le nuove sanzioni

Tra le principali novità introdotte dal regolamento vi sono i concetto di "privacy by design", con il quale s'intende la tutela del dato «fin dalla progettazione», e di "privacy by default", che concerne la tutela della vita privata «per impostazione predefinita».

Al fine di chiarire questi concetti occorre guardare, in primo luogo, al Considerando n. 78 del Regolamento, nel quale si afferma che la tutela dei diritti delle persone fisiche alla protezione dei propri dati personali richiede l'adozione di misure tecniche e organizzative adeguate e, a tal fine, «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» [56].

Alle necessità di tutela dei dati personali il titolare deve fare riferimento sin dalla 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». Inoltre, anche 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».

Ai concetti di "protezione dei dati fin dalla progettazione" e "protezione per impostazione predefinita", ancora poco chiari sia per gli operatori che per gli interpreti, è dedicato l'articolo 25 del Regolamento, il quale prevede che il titolare del trattamento, sia al momento della scelta dei mezzi tecnici per la sua gestione, sia al momento dell'acquisizione dei dati, debba mettere in atto misure tecniche e organizzative adeguate e volte ad attuare i principi in materia di protezione dei dati personali in modo efficace, «tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento».

In particolare, ai sensi del secondo comma dell'art. 25, "per impostazione predefinita", il titolare deve attuare misure che garantiscano che il trattamento sia ai dati personali necessari per ogni specifica finalità del trattamento, precisando altresì che «tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità». Inoltre, le misure devono garantire che «per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica».

Un'ulteriore importante novità introdotta dal Regolamento è rappresentata dalla cosiddetta "valutazione d'impatto", che il titolare del trattamento è tenuto a svolgere per determinare «l'origine, la natura, la particolarità e la gravità» del rischi per la tutela del diritto alla protezione del dato [57].

Essa sposta l'onere della valutazione dei rischi connessi al trattamento in capo al titolare e deve essere svolta ogni qual volta si sia in presenza di un tipo di trattamento che preveda l'utilizzo delle nuove tecnologie e che, in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento, possa presentare un "rischio elevato" per i diritti e le libertà delle persone fisiche [58].

Qualora tale "rischio elevato" sia sussistente, prima di procedere al trattamento, il titolare deve effettuare una specifica valutazione, volta a determinare quali misure organizzative e di sicurezza debbano essere adottate per rispettare quanto previsto dal Regolamento, da effettuarsi mediante analisi della «particolare probabilità e gravità del rischio, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio» [59].

Il giudizio, quindi, sul "grado di sensibilità" o di riservatezza del dato, alla luce delle possibili conseguenza nel caso in cui tale dato venisse trattato in modo non conforme al regolamento e con conseguente lesione dei diritti dei soggetti interessati, e sulle misure tecniche ed organizzative da attuare ai fini della sua protezione, è dunque, in buona parte, spostato in capo allo stesso titolare.

Spetterà, quindi, allo stesso titolare, valutare se i trattamenti presentino un rischio elevato e, in tal caso, verificare se esso può essere attenuato mediante l'attuazione di misure «opportune in termini di tecnologia disponibile e costi di attuazione» o se, in caso contrario, sia necessario consultare l'autorità di controllo.

Tale valutazione, introdotta ex novo dal Regolamento, va a sostituire il meccanismo di notificazione previsto ai sensi della Direttiva 95/46/CE [60].

Il Regolamento introduce, inoltre, una nuova figura che può, e talvolta deve, affiancare il titolare o responsabile del trattamento nell'attuazione delle misure per la protezione dei dati personali: il Data Protection Officer o responsabile

per la protezione dei dati.

Si tratta di una figura professionale obbligatoria quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico (ad eccezione delle autorità giurisdizionali, nell'esercizio di tali funzioni), ove i trattamenti richiedano il monitoraggio regolare e sistematico degli interessati su larga scala e nei casi nei quali 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'art. 9 del Regolamento o di dati relativi a condanne penali e a reati di cui all'articolo 10 del Regolamento.

Al di fuori di tali casi, e salvo l'introduzione di ulteriori ipotesi da parte del Legislatore nazionale o europeo, il Data Protection Officer non è una figura obbligatoria.

In alcuni casi, peraltro, è possibile munirsi di un Data Protection Officer "unico" per molteplici titolari o responsabili del trattamento. Ciò, in particolare, può avvenire nell'ambito di un "gruppo imprenditoriale", purché il responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento, o nell'ambito delle autorità pubbliche o organismi pubblici, che possono nominare un responsabile "unico", tenendo però conto della struttura organizzativa e delle dimensioni delle autorità pubbliche che il Data Protection Officer andrebbe a ricoprire.

Con riguardo alla scelta della persona da nominare, il Data Protection Officer può essere un dipendente del titolare o del responsabile del trattamento oppure un soggetto esterno, incaricato mediante un contratto di servizi e deve avere una conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e deve avere le capacità necessarie per assolvere i compiti di cui è investito.

Il titolare e i responsabile del trattamento sono tenuti a coinvolgerlo in tutte le questioni riguardanti la protezione dei dati personali, fornendogli tutte le risorse necessarie per assolvere i suoi compiti e per accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica. Inoltre, egli non deve ricevere alcuna istruzione per quanto riguarda l'esecuzione dei suoi compiti e non può essere rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti.

I principali compiti del responsabile, sono disciplinati all'articolo 39 del Regolamento. In primo luogo, il DPO ha la funzione di "sorvegliante" della corretta applicazione di quanto previsto dal Regolamento e dalle ulteriori disposizioni nazionali o europee in materia di protezione dei dati. Egli deve verificarne l'osservanza, anche con riferimento all'attribuzione delle responsabilità, alla sensibilizzazione e alla formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo. Inoltre, egli deve informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento dei dati, sugli obblighi derivanti da Regolamento e dalle ulteriori disposizioni nazionali o europee in materia di protezione dei dati.

È, inoltre coinvolto nella valutazione d'impatto, della quale è tenuto a sorvegliare lo svolgimento e, se richiesto, a fornire un suo parere.

Il DPO è, infine un "punto di contatto", sia per le autorità di controllo (verso le quali ha anche un obbligo di cooperazione) che per i soggetti interessati. È, infatti, il soggetto a cui sono indirizzate tutte le comunicazioni degli interessati relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.

Nell'esecuzione di tutti i suoi compiti, il DPO deve tenere in debito conto i rischi inerenti al trattamento dei dati personali, avendo riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento ed è soggetto a un obbligo di riservatezza.

Ai fini della sicurezza della protezione dei dati personali, è introdotto dal Regolamento anche, quale ulteriore elemento di novità, un obbligo di notificazione ove si verifichi un "data breach", intendendosi per tale una violazione o perdita di controllo dei dati personali trattati, meglio definita dall'articolo 4 del Regolamento come «la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non

autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati».

Come efficacemente affermato al Considerando n. 85, infatti, «una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata».

Pertanto, è stato introdotto l'obbligo di notificare le eventuali violazioni subite alle autorità Garanti «senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza», salvo che «il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche». Inoltre, la violazione dovrebbe essere comunicata alle persone interessate, qualora «sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie» [61].

Infine, con riguardo alle sanzioni applicabili in caso di violazione della normativa a tutela dei dati personali, il Regolamento ha comportato un inasprimento sanzionatorio. In particolare, con riguardo alle sanzioni amministrative pecuniarie, ai fini della determinazione del *quantum*, oltre alla natura e gravità della violazione, all'elemento psicologico, alle misure adottate per prevenire e poi attenuare il danno, ed ulteriori fattori attenuanti o aggravanti [62], altresì, ove si tratti di impresa, il fatturato annuo.

Ne deriva che le sanzioni amministrative pecuniarie applicabili alle imprese previste sono le seguenti:

- fino a 10.000 euro, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore [63];

- fino a 20.000 euro, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per le violazioni più gravi [64].

7. **Considerazioni conclusive**

In conclusione il Regolamento rafforza i diritti della persone fisiche alla tutela dei propri dati personali, integrando la disciplina preesistente, in larga parte conservata, introducendo nuovi diritti in capo ai soggetti interessati o specificando ulteriormente quelli già esistenti, ad esempio mediante la previsione delle modalità per il loro esercizio, e, al contempo, aumenta gli obblighi in capo ai titolari, nonché probabilmente la loro attuazione in ragione dell'inasprimento sanzionatorio.

La modifica alla disciplina della protezione dei dati personali introdotta non costituisce una rivoluzione rispetto all'impianto normativo precedente, ma la modifica conservandone il cuore e i principi originari, che vengono ora maggiormente dettagliati e precisati alla luce delle esigenze emerse nel ventennio trascorso dall'approvazione della Direttiva.

Con riguardo all'obiettivo dell'attuazione di una più ampia armonizzazione delle norme in materia a livello europeo, ancora incerto è l'esito della riforma, essendo ampi i margini di discrezionalità dal Regolamento affidati ai legislatori nazionali, i quali potranno esercitarli congiuntamente o, comunque, in modo analogo, o intraprendere direzioni differenti, così mantenendo le differenziazioni ad oggi presenti tra le normative nazionali e le modalità di applicazione della disciplina a tutela dei dati personali con riguardo ad alcuni peculiari aspetti e settori.

Inoltre, per quanto concerne le nuove sfide poste dai *Big Data* e dall'*Internet of things*, il Regolamento, pur prevedendo una disciplina anche ad esse applicabile, in ragione anche del lungo percorso che ha portato alla definitiva approvazione del testo, non opera un intervento peculiare significativo, il quale sarà quindi demandato a

successivi interventi specifici, europei o nazionali.

Anche con riguardo al diritto all'oblio, l'intervento operato dal Regolamento non risolve molte delle problematiche che l'attuazione di un diritto di tal genere pone in relazione ai motori di ricerca e all'attività ch'essi svolgono.

La mancanza di una regolamentazione compiuta su questi temi, pur lasciando aperte molti quesiti e dubbi interpretativi, presenta il vantaggio di non consolidare in un testo normativo regole che disciplinano situazioni neonate, le quali richiedono certamente ancora un definitivo assestamento, sia con riguardo alle peculiari necessità di tutela delle persone fisiche ch'esse pongono, sia con riguardo all'elaborazione dottrinale e giurisprudenziale di costruzioni, classificazioni e soluzioni.

Nei due anni che gli Stati membri avranno a disposizione prima dell'entrata in vigore del Regolamento, gli aspetti più delicati saranno probabilmente l'armonizzazione tra un tessuto in molti Stati già esistente e consolidato – in Italia sin dal 1996 – e un approccio alla privacy che sembra più moderno e attento alle nuove esigenze portate dal digitale e dai potenti processi di automatizzazione dei dati.

Note

[*] Il presente contributo è stato preventivamente sottoposto a referaggio anonimo affidato ad un componente del Comitato di Referee secondo il Regolamento adottato da questa Rivista.

[1] La Carta dei diritti fondamentali dell'unione europea, proclamata a Nizza nel dicembre 2000 dal Parlamento europeo, dal Consiglio e dalla Commissione e modificata nel 2007, ha acquisito dal 2009, con l'entrata in vigore del Trattato di Lisbona, l'effetto giuridico vincolante dei trattati. L'articolo 8, rubricato «Protezione dei dati di carattere personale», afferma al primo comma il diritto alla protezione dei dati personali: «Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano». Al comma successivo precisa i principi applicabili al trattamento di tali dati: «Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica». Infine, si prevede la presenza di un'autorità indipendente che garantisca il rispetto del diritto alla luce di tali principi: «Il rispetto delle regole è soggetto al controllo di un'autorità indipendente».

[2] L'art. 16 del TFUE introdotto a con il Trattato di Lisbona costituisce la base giuridica dell'intera iniziativa legislativa europea di riforma delle norme in materia di protezione dei dati personali, in quanto prima dell'entrata in vigore del trattato di Lisbona, la legislazione in materia di protezione dei dati personali era divisa tra il primo pilastro (protezione dei dati a fini privati e commerciali, soggetta al metodo comunitario) e il terzo pilastro (protezione dei dati per scopi di ordine pubblico, con decisioni prese a livello intergovernativo). Venuta meno con il Trattato la struttura dei pilastri e grazie ai nuovi poteri assunti dal Parlamento, l'art. 16 TFUE consente al Parlamento e al Consiglio di stabilire le norme in materia di protezione dei dati personali sia con riguardo relative al trattamento dei dati di carattere personale operato dalle istituzioni europee, sia con riguardo ai trattamenti operati nell'esercizio delle attività che rientrano nel campo di applicazione del diritto dell'Unione.

[3] La Direttiva 95/46/CE — recepita dal Legislatore italiano con Legge n. 675 del 31 dicembre 1996, «Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali», in vigore dal maggio 1997, e successivamente rientrata quale elemento principe del Decreto legislativo n. 196 del 30 giugno 2003, cosiddetto "Codice in materia di protezione dei dati personali", in vigore dal 1 gennaio 2004, che ha raccolto in un Testo Unico la sopravvenuta normativa creatasi in relazione a singoli e specifici aspetti del trattamento dei dati, riordinando la materia — costituisce il testo europeo di riferimento in materia di protezione dei dati personali ed è volta a definire un quadro normativo che equilibri e bilanci la protezione della vita privata delle persone e la libera circolazione dei dati. È tale Direttiva che ha stabilito i principi fondanti la disciplina del trattamento dei dati personali, nonché ha istituito le Autorità garanti nazionali ed europee.

[4] Il “mercato unico digitale” è uno degli obiettivi che l’Unione europea si è posta e per l’attuazione del quale le istituzioni europee stanno introducendo importanti interventi normativi. Consiste nella creazione di un mercato unico in tutto il territorio dell’unione, ovvero nell’eliminazione delle barriere e degli ostacoli che impediscono o riducono le operazioni economiche, in prevalenza lo scambio di servizi, tra imprese appartenenti a differenti Stati membri. Sinteticamente può essere definito come l’eliminazione delle barriere nazionali alle transazioni che si svolgono on line all’interno dell’Unione, col fine ultimo di aumentare la prosperità economica e contribuire a un’unione sempre più stretta e effettiva tra gli Stati membri. Tra le azioni a tal fine intraprese vi è il programma definito nell’ambito dell’Agenda digitale europea, parte della strategia Europa 2020, che ha riconosciuto il ruolo fondamentale delle nuove tecnologie dell’informazione e della comunicazione, e ha reso la realizzazione del mercato unico digitale una priorità per le istituzioni europee. La strategia elaborata dalle istituzioni poggia su tre pilastri: 1) Migliorare l’accesso ai beni e servizi digitali in tutta Europa per i consumatori e le imprese; 2) Creare un contesto favorevole e parità di condizioni affinché le reti digitali e i servizi innovativi possano svilupparsi; 3) Massimizzare il potenziale di crescita dell’economia digitale.

[5] Le consultazioni si sono svolte nell’arco di oltre due anni, ricomprendenti consultazioni ad hoc con i principali portatori di interessi e due fasi di consultazione pubblica: dal 9 luglio al 31 dicembre 2009 in relazione al quadro giuridico del diritto fondamentale alla protezione dei dati personali (168 risposte, 127 provenienti da privati cittadini, organizzazioni e associazioni imprenditoriali e 12 dalle autorità pubbliche); dal 4 novembre 2010 al 15 gennaio 2011 sulla comunicazione della Commissione «Un approccio globale alla protezione dei dati personali nell’Unione europea» (305 risposte, 54 da privati cittadini, 31 da autorità pubbliche e 220 da organizzazioni private, soprattutto associazioni d’imprese e organizzazioni non governative).

[6] Cfr. COM(2010) 609 definitivo, «Un approccio globale alla protezione dei dati personali nell’Unione europea».

[7] Cfr. COM(2012) 11 final 2012/0011 (COD), disponibile al seguente link: http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52012PC0011&from=IT [16.04.2016].

[8] Tra i passi più importanti si ricorda: la Risoluzione legislativa del Parlamento europeo del 12 marzo 2014 sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), disponibile al seguente link http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=IT&ring=A7-2013-0402 , mediante la quale il Parlamento ha introdotto numerose ed importanti modifiche al testo originario; il 15 giugno 2015 il Consiglio Giustizia e Affari Interni ha adottato un Orientamento Generale sul Regolamento, disponibile al seguente link http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/it/pdf; nel giugno 2015 si sono tenuti i negoziati, che hanno portato all’accordo solo nel dicembre 2015.

[9] Cfr. Articolo 2 del Regolamento, non dissimile dalla previsione già contenuta nella Direttiva 95/46/CE.

[10] Trattasi delle politiche relative ai controlli alle frontiere, all’asilo e all’immigrazione.

[11] Il considerando n. 19 prevede, infatti quanto segue: «La protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro, e la prevenzione di, minacce alla sicurezza pubblica, e la libera circolazione di tali dati sono oggetto di uno specifico atto dell’Unione. Il presente regolamento non dovrebbe pertanto applicarsi ai trattamenti effettuati per tali finalità. […]».

[12] Ai sensi del considerando n. 20, infatti: «Quando il trattamento dei dati personali effettuato da organismi privati rientra nell’ambito di applicazione del presente regolamento, è opportuno che lo stesso preveda la facoltà per gli Stati membri, a determinate condizioni, di adottare disposizioni legislative intese a limitare determinati obblighi e diritti, qualora tale limitazione costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia di importanti interessi specifici, comprese la sicurezza pubblica e le attività di prevenzione, indagine,

accertamento e perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro, e la prevenzione di, minacce alla sicurezza pubblica. Ciò riveste particolare importanza ad esempio nel quadro del riciclaggio o di attività di medicina legale».

[13] Cfr. art. 2, quarto comma, e considerando n. 21.

[14] Ove la Direttiva prevedeva, invece, «qualsiasi informazione concernente una persona fisica identificata o identificabile («persona interessata»); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale».

[15] Ove la definizione fornita dalla Direttiva prevedeva invece: «qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione».

[16] Di nuova introduzione sono, inoltre, le definizioni di: "limitazione del trattamento", "violazione dei dati personali", "dati genetici", "dati biometrici, "dati relativi alla salute", "stabilimento principale", "rappresentante", "impresa; "gruppo imprenditoriale", "norme vincolanti d'impresa", "autorità di controllo", "autorità di controllo interessata", "trattamento transfrontaliero", "obiezione pertinente e motivata", "servizio della società dell'informazione", "organizzazione internazionale". Permangono, rispetto al testo della Direttiva, seppur con qualche intervento, le definizioni di "archivio", "titolare del trattamento" («la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali»), "responsabile del trattamento" («la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento»), "destinatario", "consenso dell'interessato".

[17] Inoltre, nel motivare tale decisione il Garante ha dichiarato quanto segue: «Le precedenti versioni italiane del Regolamento, infatti, riportavano i termini "responsabile del trattamento" (data controller) e "incaricato del trattamento" (data processor). Tuttavia, trattandosi, di fatto, di figure identiche quanto a caratteristiche soggettive a quelle che nel Codice Privacy italiano sono indicate rispettivamente come "titolare" e "responsabile", l'Autorità italiana ha chiesto ed ottenuto che i nuovi testi mantenessero tali diciture in modo da evitare a imprese, enti, professionisti e cittadini ogni possibile problema di interpretazione giuridica ed eventuali costi, anche materiali, connessi al cambiamento terminologico».

[18] Cfr. Art. 5, primo comma, lett. a) del Regolamento.

[19] Cfr. Art. 5, primo comma, lett. b) del Regolamento.

[20] Cfr. Art. 5, primo comma, lett. c) del Regolamento.

[21] Cfr. Art. 5, primo comma, lett. d) del Regolamento, il quale precisa altresì che «devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati».

[22] Cfr. Art. 5, primo comma, lett. e) del Regolamento, il quale prevede, inoltre, che «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».

[23] Cfr. Art. 5, primo comma, lett. f) del Regolamento, il quale precisa altresì che la sicurezza ricomprende «la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla

perdita, dalla distruzione o dal danno accidentali».

[24] Agli Stati membri, ai sensi del secondo comma del medesimo articolo, è consentito di specificare ulteriormente l'elencazione, mediante il mantenimento o l'introduzione di norme più specifiche.

[25] Cfr. Art. 7 del Regolamento. L'art. 8 successivo, è dedicato al consenso prestato da soggetti minori, rubricato «Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione» prevede la liceità del trattamento dei dati personali del minore, basato sul suo consenso di questi, soltanto ove egli abbia compiuto il sedicesimo anno di età (che gli Stati membri possono decidere di abbassare sino al tredicesimo anno); in caso contrario il consenso deve essere prestato o autorizzato dal titolare della responsabilità genitoriale. L'articolo impone, inoltre al titolare del trattamento un obbligo di adoperarsi per verificare «in modo ragionevole» e «in considerazione delle tecnologie disponibili» che il consenso, anche del minore, sia validamente prestato.

[26] Cfr. Art. 7, terzo comma, il quale specifica altresì che le modalità da impiegarsi per l'attuazione del diritto di revoca non possono comportare un compito gravoso per l'interessato, affermando anzi che «Il consenso è revocato con la stessa facilità con cui è accordato».

[27] Cfr. Art. 12 del Regolamento, ove è ulteriormente precisato che le informazioni possono essere fornite sia per iscritto che con mezzi elettronici, oltre che, se richiesto dall'interessato, anche oralmente, «purché sia comprovata con altri mezzi l'identità dell'interessato».

[28] Termine prorogabile a due mesi se «necessario, tenuto conto della complessità e del numero delle richieste», informando l'interessato della proroga e dei motivi che hanno determinato il ritardo.

[29] Ai sensi dell'art. 12 del Regolamento, quinto comma, il titolare del trattamento può rifiutarsi di soddisfare le richieste di cui agli artt. da 15 a 20 del Regolamento, qualora esse siano «manifestamente infondate o eccessive» o, in alternativa, può «addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta».

[30] Il primo comma prevede che siano fornite le informazioni seguenti: «a) l'identità e i dati di contatto del titolare del trattamento e, eventualmente, del suo eventuale rappresentante; b) i dati di contatto del responsabile della protezione dei dati, ove applicabile; c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi; e) gli eventuali destinatari o le categorie di destinatari dei dati personali; f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili». Ai sensi del secondo comma dell'art. 13, all'interessato devono, inoltre, essere fornite le seguenti informazioni: «a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; d) il diritto di proporre reclamo a un'autorità di controllo; e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati; f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato».

[31] Ai sensi dell'art. 14 del Regolamento devono, infatti essere fornite le seguenti informazioni: «a) l'identità e i dati di contatto del titolare del trattamento e del suo eventuale rappresentante; b) i dati di contatto del responsabile della protezione dei dati, ove applicabile; c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; d) le categorie di dati personali in questione; e) i destinatari o le categorie di destinatari dei dati personali se del caso; e f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili». Nonché, specularmente a quanto già descritto in relazione al trattamento per il quale i dati siano raccolti presso l'interessato: «a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; b) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi; c) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; d) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca; e) il diritto di proporre reclamo a un'autorità di controllo; f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico; g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato».

[32] Nel caso in cui i dati siano destinati alla comunicazione all'interessato o a un altro soggetto, le informazioni all'interessato relative al trattamento devono essere fornite al più tardi entro il momento della comunicazione.

[33] Cfr. Art. 14, quinto comma, del Regolamento.

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

[35] Ovvero ove vi sia «un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge».

[36] Inoltre, «qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento».

[37] Cfr. Art. 20 del Regolamento.

[38] Cfr. Considerando n. 68 del Regolamento.

[39] L'art. 8 della Direttiva, dedicato ai «trattamenti riguardanti categorie particolari di dati", prevedeva, infatti, il divieto di trattare "dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento di dati relativi alla salute e alla vita sessuale», il quale non si applicava qualora: «a) la persona interessata abbia dato il proprio consenso esplicito a tale trattamento, salvo nei casi in cui la legislazione dello Stato membro preveda che il consenso della persona interessata non sia sufficiente per derogare al divieto di cui al paragrafo 1, oppure b) il trattamento sia necessario, per assolvere gli obblighi e i diritti specifici del responsabile del trattamento in materia di diritto del lavoro, nella misura in cui il

trattamento stesso sia autorizzato da norme nazionali che prevedono adeguate garanzie, oppure c) il trattamento sia necessario per salvaguardare un interesse vitale della persona interessata o di un terzo nel caso in cui la persona interessata è nell'incapacità fisica o giuridica di dare il proprio consenso; o d) il trattamento sia effettuato, con garanzie adeguate, da una fondazione, un'associazione o qualsiasi altro organismo che non persegua scopi di lucro e rivesta carattere politico, filosofico, religioso o sindacale, nell'ambito del suo scopo lecito e a condizione che riguardi unicamente i suoi membri o le persone che abbiano contatti regolari con la fondazione, l'associazione o l'organismo a motivo del suo oggetto e che i dati non vengano comunicati a terzi senza il consenso delle persone interessate; o e) il trattamento riguardi dati resi manifestamente pubblici dalla persona interessata o sia necessario per costituire, esercitare o difendere un diritto per via giudiziaria».

[40] Cfr. Art. 4 del Codice Privacy.

[41] Ai sensi del secondo comma dell'art. 46 del Codice, «il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione, ovvero successivamente, anche sulla base di eventuali verifiche, il Garante può prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare».

[42] Cfr. art. 4 e Considerando n. 72 del Regolamento.

[43] Cfr. Considerando n. 60 del Regolamento.

[44] Cfr. Considerando n. 71 del Regolamento e, più ampiamente, l'art. 22 del Regolamento, rubricato «Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione», il quale prevede, al primo comma, quanto segue: «L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona».

[45] Cfr. Considerando n. 71 del Regolamento.

[46] Cfr. Considerando n. 71 del Regolamento.

[47] Disponibili al seguente link: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3881513.

[48] Con riguardo ai cookies, ad esempio, il considerando n. 25 della Direttiva 2002/58/CE afferma che, «allorché tali dispositivi, ad esempio i marcatori ("cookies"), sono destinati a scopi legittimi, come facilitare la fornitura di servizi della società dell'informazione, il loro uso dovrebbe essere consentito purché siano fornite agli utenti informazioni chiare e precise, a norma della direttiva 95/46/CE, sugli scopi dei marcatori o di dispositivi analoghi per assicurare che gli utenti siano a conoscenza delle informazioni registrate sull'apparecchiatura terminale che stanno utilizzando», precisando altresì che «gli utenti dovrebbero avere la possibilità di rifiutare che un marcatore o un dispositivo analogo sia installato nella loro apparecchiatura terminale».

[49] Da ultimo, modificata dal decreto legislativo 28 maggio 2012, n. 69 «Modifiche al decreto legislativo 30 giugno 2003, n. 196, recante Codice in materia di protezione dei dati personali in attuazione delle direttive 2009/136/CE, in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche, e 2009/140/CE in materia di reti e servizi di comunicazione elettronica e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori».

[50] Cfr. Considerando n. 59 del Regolamento.

[51] Ai sensi del Considerando n. 59, «in particolare qualora i dati personali siano trattati con mezzi elettronici».

[52] Sul punto, il Considerando n. 66, specificando quanto previsto all'art. 17, prevede quanto segue: «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».

[53] Cfr. Considerando n. 65 e art. 17, terzo comma, del Regolamento.

[54] Cfr. Articolo 21, primo comma, del Regolamento.

[55] Cfr. Articolo 21, primo comma, del Regolamento.

[56] Vi è poi un’elencazione delle misure che potrebbero essere in concreto attuate a tal fine dal titolare del trattamento: «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».

[57] Cfr. Considerando n. 84 del Regolamento.

[58] Cfr. Articolo 35, primo comma, del Regolamento.

[59] Cfr. Considerando n. 90 e art. 35, settimo comma, del Regolamento.

[60] In tal senso, cfr. Considerando n. 89.

[61] Cfr. Considerando n. 86 del Regolamento.

[62] Cfr. art. 83. del Regolamento, il quale elenca dettagliatamente gli elementi da valutarsi ai fini della determinazione.

[63] In caso di violazione di: «a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 e 43; b) gli obblighi dell’organismo di certificazione a norma degli articoli 42 e 43; c) gli obblighi dell’organismo di controllo a norma dell’articolo 41, paragrafo 4».

[64] Applicabile in caso di: «a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9; b) i diritti degli interessati a norma degli articoli da 12 a 22; c) i trasferimenti di dati personali a un destinatario in un paese terzo o un’organizzazione internazionale a norma degli articoli da 44 a 49». Nonché per «l’inosservanza di un ordine da parte dell’autorità di controllo di cui all’articolo 58, paragrafo 2».

31 maggio 2016