Dipartimento di Giurisprudenza

Cattedra di Informatica Giuridica

LA PROTEZIONE DEI DATI PERSONALI: L'IMPATTO DEL GDPR SUGLI STATI MEMBRI DELL'UNIONE EUROPEA

RELATORE

Chiar.mo Prof. Francesco Romeo

CANDIDATO

Luca Esposito

MATRICOLA

115033

CORRELATORE

Chiar.mo Prof. Fabio Bartolomeo

ANNO ACCADEMICO 2017/2018

La protezione dei dati personali: l'impatto del GDPR sugli Stati membri dell'Unione Europea

Indice

INTRODUZIONE

Introduzione

La *privacy*, come viene continuamente sottolineato, rappresenta oggi la base identitaria su cui ciascuno di noi edifica liberamente la propria personalità ed è sicuramente uno dei principi cardine su cui fondare una riorganizzazione delle società nell'epoca della globalizzazione e dell'informazione. Le nuove dimensioni della raccolta e del trattamento delle informazioni personali, la pervasività del controllo che oggi è possibile operare sulle persone, da parte di soggetti sia pubblici che privati, ha provocato la moltiplicazione della richiesta di tutela e la consapevolezza dell'impossibilità di circoscrivere le relative problematiche nel quadro tradizionale. Oggi, infatti, il centro di gravità è sempre più individuato, più che nel diritto di essere lasciati soli, nella possibilità di ciascuno di noi di controllare l'uso delle informazioni che lo riguardano e nel considerare i problemi della *privacy* nel quadro dell'attuale organizzazione del potere, di cui appunto l'infrastruttura informativa rappresenta ormai una delle componenti fondamentali. Di fronte all'esigenza sempre più avvertita di norme giuridiche chiare e coerenti, condivise ed efficaci, ci si trova spesso davanti ad un vero proprio disorientamento giuridico, in cui le stesse categorie tradizionali (come ad esempio la dignità della persona, l'autodeterminazione individuale, il diritto alla salute, etc.) subiscono un effetto di spiazzamento e riformulazione. Il concetto di *privacy*, così sfuggente ad ogni definizione che possa dirsi completamente esaustiva, viene sempre più accostato alla persona, come mezzo per tutelare la sua dignità e il suo sviluppo all'interno della società.

Questa premessa risulta necessaria per comprendere come ormai si possa parlare di *privacy* per quanto riguarda qualsiasi tipo di attività quotidiana e qualsiasi relazione all'interno di una società moderna. Ma, naturalmente, il concetto di *privacy*, così come concepito attualmente, ha poco in comune con quello sviluppatosi secoli fa. Ed è questo il fulcro del presente elaborato, il cui obiettivo è quello di mostrare quanto ed in che modo si sia evoluto il concetto di

privacy, che può tradursi in italiano con i termini di riservatezza o privatezza, diritti fondamentali di ogni persona.

Nel primo capitolo si analizzerà lo sviluppo storico del concetto di *privacy* dalla sua nascita ai giorni nostri. La prima elaborazione di tale concetto viene fatta risalire al 1890, grazie ad un saggio pubblicato da due giuristi americani, Samuel Warren e Louis Brandeis, "*The Right to Privacy*". Fino ad allora, la riservatezza veniva vista come un diritto che poteva appartenere solo a pochi, nonché un diritto recante solo una connotazione negativa, consistente nel diritto ad essere lasciati soli. In America il diritto alla riservatezza si è sviluppato sempre più grazie all'apporto prima dei due giuristi sovra menzionati, poi per le numerose sentenze che hanno plasmato il diritto in esame in base alle esigenze avvertite dalla società. Fra tutte, verranno analizzate le sentenze "*Olmstead vs. United States*" del 1928 e "*Katz vs. United States*" del 1967, entrambe aventi ad oggetto intercettazioni effettuate senza autorizzazione; la prima resterà nella storia soprattutto per la "*dissenting opinion*" di Louis Brandeis, nel frattempo divenuto giudice della Corte Suprema, la seconda verrà ricordata invece per la "*concurring opinion*" del giudice Harlan.

Dopo aver ripercorso lo sviluppo storico nel panorama americano l'analisi si sposterà sul versante europeo ed in particolar modo su quello italiano. In Europa, parallelamente al periodo dei primi codici civili della storia, si sviluppò un importante filone in materia di *privacy* che venne disciplinata pressochè in ogni Stato membro. Successivamente la materia è stata oggetto di attenzione e di studio anche a livello comunitario, in particolar modo grazie alla Direttiva 95/46/CE, la quale fece da battistrada per tutte le successive discipline locali. Naturalmente una normativa fu emanata anche in Italia, ovvero il D.Lgs. 196/2003, meglio conosciuto come Codice della Privacy, tutt'ora vigente e recentemente rinominato Nuovo Codice della Privacy, per effetto del D.Lgs. 101/2018.

Nel secondo capitolo del presente elaborato verrà analizzato il principale oggetto di studio preso in esame, il nuovo Regolamento europeo in materia di protezione dei dati personali, meglio conosciuto come GDPR (General Data

Protection Regulation), numero 679 del 2016. Questo capitolo centrale sarà dedicato ad un'approfondita analisi del testo del Regolamento che, nonostante recepisca molte disposizioni già emanate in passato, detta anche innumerevoli nuove regole in materia di protezione dei dati. L'intento principe del nuovo Regolamento UE è sicuramente quello di armonizzare e uniformare la disciplina comunitaria, così che non si creino più discrepanze tra le varie normative locali. Il presente Regolamento è entrato ufficialmente in vigore in data 25 maggio 2018, è composto da 173 considerando, premessi al testo della disposizione, e 99 articoli, suddivisi in undici capi. Ogni capo sarà oggetto di un'attenta disamina, e ove possibile, di una comparazione con la normativa europea previgente rappresentata per la maggior parte dalla Direttiva 95/46/CE, ormai abrogata.

Il terzo ed ultimo capitolo dell'elaborato sarà incentrato su una comparazione tra la disciplina dettata dal Codice della Privacy del 2003 e il Regolamento del 2018. Il Codice della Privacy resta tutt'ora in vigore, ma è stato recentemente adattato alla disciplina del GDPR dal D.Lgs. 101/2018. Il capitolo analizzerà le differenze intercorrenti tra la disciplina italiana e quella comunitaria e, laddove sia possibile, si analizzerà anche quello che è stato il frutto dell'adattamento ad opera del decreto 101.

L'obiettivo ultimo di questo scritto è quello di mostrare come nel corso degli anni, o meglio dei secoli, la disciplina in materia di riservatezza e protezione dei dati personali si sia evoluta sempre di più, vista anche la crescita dei mezzi attraverso i quali avviene la circolazione dei dati personali. Oramai esistono innumerevoli canali di circolazione per i nostri dati, e spesso è anche difficile controllarne il flusso o la portata. Lo scopo delle varie normative è quello di adattarsi sempre di più alle esigenze della società sulla quale sono parametrate le disposizioni.

CAPITOLO 1

IL CONCETTO DI PRIVACY NEL TEMPO ED EVOLUZIONE DELLA RELATIVA DISCIPLINA

Il concetto di privacy nel tempo ed evoluzione della relativa disciplina

Il termine *privacy*, utilizzato in italiano anche col corrispettivo riservatezza[1], apparentemente sembra un concetto sociologico di semplice ed immediata captazione all'individuo comune. In realtà, in virtù dei suoi risvolti principalmente informatici che coinvolgono oggigiorno chiunque interagisca in modo preponderante con strumenti quali Internet, computer, smartphone e via dicendo, nasconde un'evoluzione non solo storico-giuridica, ma anche, per l'appunto, storico-sociale, che infonde le sue radici in epoche molto antiche.

Dunque fin dall'antichità l'uomo ha avvertito la necessità di ritagliarsi spazi per sé stesso al fine di proteggere la propria sfera privata ed evitare informazioni inutili e pettegolezzi. Col tempo la riservatezza ha incominciato ad assumere una rilevanza così particolare tale da separare la vita pubblica da quella privata.

La ricerca della riservatezza si è evoluta in maniera direttamente proporzionale all'evoluzione dell'uomo stesso e della società nella quale egli si trovava. In origine era una mera protezione fisica, dettata dalla necessità di difendersi dalle intemperie e dagli animali, nell'antica Grecia era una separazione della vita familiare dalla vita pubblica, nella Roma di Giulio Cesare[2] era invece un modo per non diffondere informazioni agli schieramenti nemici.

Probabilmente, la posizione più autorevole è rinvenibile nell'antica Grecia da parte del celebre filosofo di Stagira, Aristotele. Aristotele propone, in una delle sue opere più illustri, "La Politica", una distinzione ormai classica fra la sfera

[1] Questa posizione tuttavia non è pacifica. Dal punto di vista prettamente linguistico, riservatezza è tradotto in inglese come "*confidentiality*", intendendolo in modo più ampio del termine *privacy*. Dal punto di vista giuridico invece spesso si parla di privacy, riservatezza e tutela dei dati personali come sinonimi. Tuttavia, è più corretto considerarli come fossero facciate della stessa piramide piuttosto che come semplici significati equivalenti.

[2] In crittografia il "cifrario di Giulio Cesare" è uno dei più antichi algoritmi crittografici di cui si abbia traccia storica. È un cifrario a sostituzione monoalfabetica in cui ogni lettera del testo in chiaro è sostituita nel testo cifrato dalla lettera che si trova un certo numero di posizioni dopo nell'alfabeto. Al tempo era un metodo sicuro perché gli avversari non erano neanche in grado di leggere un testo in chiaro, men che mai uno cifrato.

pubblica, connessa all'attività politica intesa col corrispondente greco di "*Polis*"[3], e la sfera privata, "*Oikos*"[4], associata alla famiglia ed alla vita domestica. In questo modo viene individuato un ambito personale e familiare come un'entità distaccata ma soprattutto tutelata rispetto all'ambito pubblico e politico dalla quale si comincia a prendere le distanze.

Sulle stesse note di questa posizione, sempre in Grecia, anche il celeberrimo drammaturgo ateniese, Sofocle, propone nella sua opera "Antigone", in modo sorprendentemente attuale, una netta distinzione fra sfera pubblica e sfera privata, che si ripercuote alla luce della distinzione fra diritto positivo e diritto naturale. Questa tragedia[5] rappresenta un vero e proprio punto di partenza non solo sociale ma anche giuridico per l'affermazione della libertà personale alla luce del diritto naturale opposto alle ferree leggi dello Stato del diritto positivo.

1.1 Origine del concetto di privacy

L'evoluzione di un simile concetto ha portato a quel che oggi si definisce "*privacy*", la cui origine si fa risalire, tradizionalmente, a due giuristi statunitensi, Samuel Warren e Louis Brandeis, i quali diedero alle stampe un saggio intitolato *"The Right to Privacy. The Implicit Made Explicit."*[6], pubblicato nell'anno 1890. I due giovani avvocati di Boston preparavano una causa contro le indiscrezioni sulla vita matrimoniale della moglie dello stesso Warren, da parte di uno dei primi

[3] "*Πόλις*".
[4] "*Οἶκος*".
[5] Tale opera, forse punta di diamante fra le tragedie sofoclee, racconta la storia di Antigone, che decide di dare sepoltura al cadavere del fratello Polinice contro la volontà del nuovo re di Tebe, Creonte. Scoperta, viene condannata dal re a vivere il resto dei suoi giorni imprigionata in una grotta, nella quale poi si impicca. Questo porta al suicidio del figlio di Creonte, Emone, promesso sposo di Antigone, e poi della moglie dello stesso re, Euridice, lasciando il solo Creonte a maledire la propria stoltezza. Le azioni della protagonista, che nascono nella sua coscienza come diritto naturale, si contrappongono alle leggi positive di Creonte, che negano la sepoltura del fratello così come la sfera privata dell'*Oikos* comincia a staccarsi dalla sfera pubblica della *Polis* greca.
[6] *The Right to Privacy*, Samuel Warren and Louis Brandeis, 1890, *Harvard Law Review*.

giornali che utilizzava la macchina da stampa rotativa[7], la "*Boston Evening Gazette*".

I due avvocati si ritrovarono, quindi, a riflettere su quali informazioni riguardanti la vita personale di un individuo dovessero essere di pubblico dominio e quali, invece, meritassero una tutela dall'invadenza altrui. La pubblicazione dei due avvocati fu il primo scritto di carattere giuridico in assoluto a riconoscere l'esistenza di un autonomo diritto alla *privacy*, meglio definito come "the right to be let alone", ossia il "diritto di essere lasciato solo"[8]. Diversamente da come si può facilmente dedurre, il "right to be let alone" non consiste in un'astratta aspirazione della persona ad essere lasciata sola, ma va inteso piuttosto come il desiderio di non vedersi violata la propria intimità, unito all'esigenza di tranquillità almeno tra le mura domestiche della propria vita privata.

L'intento di Warren e Brandeis fu quello di tutelare, attraverso il diritto alla *privacy*, gli aspetti più intimi e riservati dell'uomo, proteggendo oltre al valore fondamentale della proprietà privata quello dell'inviolabilità della sfera personale, costituita da elementi di comportamento e di vita privata. Essi focalizzarono l'attenzione sull'esigenza di una protezione giuridica della personalità di ogni individuo, e l'esito che ottennero fu chiaramente positivo.

Tuttavia, la *privacy*, nella sua fase primordiale, assume sostanzialmente un carattere negativo[9], in quanto il diritto ad essere lasciati soli esprime la necessità della persona di eliminare, o quantomeno escludere, l'ingerenza di soggetti esterni nella propria sfera privata, generandola dunque come "libertà da" piuttosto che "libertà di".

---

[7] La rotativa è una macchina per la stampa nella quale le immagini da stampare sono incurvate intorno ad un cilindro. La stampa può essere effettuata su diversi tipi di supporti: carta, cartone e plastica, in fogli o su rulli continui.

[8] Tuttavia, il termine "*to be let alone"* è stato usato per la prima volta dal giudice T.M. Cooley, in "*Treatise on the law of Torts or the Wrongs Which Arise Independently of Contract*", del 1878, pubblicato da *Callaghan e Company*, 1907.

[9] L'interpretazione data dai sopracitati giuristi alla nozione, concepisce la *privacy* come una delle c.d. "*libertà negative*" tipiche degli stati liberali, intese come strumento di tutela della sfera di autonomia del singolo dall'ingerenza dei pubblici poteri.

La *privacy*, infatti, per via del contesto storico, economico e sociale in cui viene concepita, viene intesa in termini di riservatezza come "tipico diritto della borghesia" che, in un contesto sociale come quello di fine Ottocento, avverte il bisogno di tutelare i propri spazi vitali da possibili intrusioni esterne.

Venendo al significato più profondo attribuito a questo diritto, Warren e Brandeis asserivano che si trattasse di un concetto rintracciabile all'interno di un principio già insito al sistema di Common Law che andava a tutelare l'area privata del singolo, inteso come quello spazio domestico nel quale ognuno poteva fare quel che desiderava, pensare senza ingerenze, al riparo da occhi ed orecchie altrui.

Si trattava dell'istituto giuridico della proprietà privata, inteso a quell'epoca, secondo una concezione molto in voga e cara al modello liberale, come l'apposizione di chiusure e steccati per non permettere agli altri di subentrare nel proprio terreno, espresso col termine latino "*ius excludendi alios*". In questo modo, per gli autori, il diritto alla *privacy* è un concetto essenziale che sottace alla ricerca della felicità, riconosciuto come diritto fondamentale della cultura statunitense, nonché baluardo della stessa Costituzione Americana.

È evidente come, così delineato, il concetto di *privacy* assume una componente completamente negativa, intesa come quel diritto di non voler intrusioni nella propria sfera privata, così come anticipato in precedenza.

Il diritto alla riservatezza inteso nel saggio è costruito con prevalente riferimento alla classe sociale medio-alta all'interno dei ceti sociali dell'epoca. La rivoluzione tecnologica, dal punto di vista della tutela della riservatezza, colpì quasi esclusivamente la classe aristocratica che, a quel tempo, si sentiva ancora legata ad un forte sentimento di intangibilità nei confronti delle classi sociali inferiori e che dunque poteva ritenersi offesa da violazioni alla loro *privacy* a dispetto di quest'ultime.

In questo senso, il diritto alla *privacy* sebbene nasca nell'epoca borghese, si origina come un diritto dei ricchi, degli aristocratici, di quel ceto descritto come

"*ancien régime*". Sarà proprio Brandeis[10] a far evolvere ulteriormente il diritto alla riservatezza ad un livello successivo, così da scavalcare nuovamente quelle catene e consentire progressivamente il raggiungimento di un nuovo e più ampio livello di tutela[11].

1.1.1 Il Quarto Emendamento della Costituzione americana e la *dissenting opinion* del giudice Brandeis.

Per poter meglio apprezzare questa evoluzione del diritto alla riservatezza, dovuta a Brandeis, bisogna prima fare un breve accenno sulla Costituzione Americana.

La Costituzione Americana, legge suprema degli Stati Uniti d'America, fu completata nel 1787 ed entrò in vigore nel 1789. Essa pone le sue radici nella lontana "*Magna Charta Libertatum*" britannica del 1215 e nel "*Bill of Rights*"[12], che aggiunse Dieci Emendamenti nel 1791.

All'interno di questa Carta, è di fondamentale importanza, per il nostro studio, il Quarto Emendamento. Esso non prevede un espresso riferimento al diritto alla *privacy* nei confronti del cittadino americano, tuttavia, ciò non impedisce comunque di ritenere che la *privacy* sia un bene giuridico costituzionalmente tutelato. Esso recita: "Il diritto dei cittadini ad essere al sicuro nelle loro persone, case, documenti ed effetti contro perquisizioni e sequestri non ragionevoli, non potrà essere violato, e non potranno essere emessi mandati se non

[10] Infatti, sebbene Brandeis e Warren vengano ricordati entrambi per il loro apporto sul tema qui trattato, solo Brandeis rimane anche in seguito al centro del dibattito sul diritto alla riservatezza, tanto da diventare addirittura giudice di Corte Suprema, approfondendo ulteriormente il tema della rilevanza dell'evoluzione tecnologica in contrapposizione all'individuo.

[11] L. Miglietti, *Profili storico-comparativi del diritto alla privacy*, Diritti Comparati, 2014.

[12] Si tratta per l'appunto di un documento contenete i primi dieci emendamenti della Costituzione Americana; furono introdotti da parte di James Madison, riconosciuto come uno dei "*fathers of Constitution*" e quarto Presidente degli Stati Uniti d'America. Furono stilati prendendo spunto dalla Dichiarazione dei Diritti proclamata in Virginia, nel 1776.

su motivi fondati, sostenuti da giuramenti o solenni affermazioni e con una dettagliata descrizione del luogo da perquisire e delle persone o cose da prendere in custodia"[13].

Come è evidente, manca un espresso riferimento ad un diritto alla riservatezza nel menzionato Emendamento, tuttavia, agli occhi di un lettore moderno, non è certo possibile non rintracciare almeno una scia, un sentore, del concetto di *privacy* quantomeno a livello embrionale.

Come già anticipato in precedenza, uno dei primi giuristi ad accogliere una lettura moderna di questo tipo, fu proprio Luis Brandeis, diventato nel contempo giudice supremo, nella sua celebre *dissenting opinion* nella causa "*Olmstead vs. United States*" del 1928[14]. Si trattò del primo caso nella storia della Corte Suprema degli Stati Uniti di intercettazioni telefoniche. La questione verteva su una presunta violazione del Quarto Emendamento, commessa dagli agenti FBI nei confronti del soggetto Roy Olmstead[15].

La Corte in questo caso ha esaminato se l'uso di intercettazioni telefoniche private effettuato da agenti federali senza approvazione giudiziaria e successivamente utilizzato come prova costituisse una violazione dei diritti del convenuto previsti dal Quarto Emendamento. Le prove fornite in seguito alle intercettazioni telefoniche rivelarono una cospirazione di straordinaria magnificenza finalizzata al contrabbando, coinvolgendo una cinquantina di persone, l'utilizzo di navi marittime per il trasporto, un deposito sotterraneo a Seattle e il mantenimento di un ufficio centrale completamente attrezzato, grazie alla presenza di dirigenti, contabili, venditori e un avvocato. Secondo approfonditi

[13] "*The right of the people to be secure in their persons, houses, papers, and effects, against unresonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particulary describing the place to be searched, and the persons or things to be seized*".

[14] *Olmstead vs United States*, U.S. Supreme Court, 277 U.S. 438, 1928.

[15] Nel presente caso, Roy Olmsteas aveva organizzato un'attività illegale organizzata di contrabbando di alcol. L'attività era molto ben sviluppata, soprattutto grazie alle innumerevoli linee telefoniche che permettevano il coordinamento fra i vari complici. Le prove raccolte a danno di Olmstead furono ottenute grazie ad intercettazioni telefoniche predisposte dagli agenti dell'FBI, ma senza alcuna richiesta di mandato per effettuarle, in quanto non era avvenuta nessuna violazione fisica di uffici o abitazioni personali.

studi, anche in un mese negativo le vendite ammontavano a circa $176.000. Olmstead era l'artefice di tutto questo, ricevendo la metà di tutti i profitti. Le informazioni che hanno portato alla scoperta del suo coinvolgimento e della stessa cospirazione sono state in gran parte ottenute da quattro funzionari federali che sono stati in grado di intercettare messaggi sui telefoni di Olmstead e altri cospiratori. Nessuna legge è stata violata nell'installare l'attrezzatura per le intercettazioni telefoniche, poiché gli ufficiali non hanno violato le case o gli uffici degli imputati; l'attrezzatura è stata collocata nelle strade vicino alle case e nel seminterrato del grande edificio per uffici. Le intercettazioni sono continuate per diversi mesi e le registrazioni hanno rivelato dettagli significativi sulle transazioni commerciali effettuate. Furono fatte annotazioni stenografiche delle conversazioni e la loro accuratezza fu confermata più volte durante il processo; le prove rivelavano tutti i dettagli delle operazioni e mostravano anche la relazione tra Olmstead e alcuni membri della polizia di Seattle, che hanno portato al rilascio immediato di alcuni membri della cospirazione arrestati e a numerose promesse nei confronti degli ufficiali di polizia.

Il giudice capo William Howard Taft ha espresso il parere della Corte, elencando gli emendamenti rilevanti nel caso concreto e esaminando i precedenti in questione. Un primo importante precedente fu "*Boyd vs. United States*"[16], il quale riguardava una legge americana del 1874, che prevedeva la possibilità di utilizzare un maresciallo per ottenere prove che il convenuto si era rifiutato di fornire. La Corte riteneva che la legge del 1874 costituisse una violazione del Quarto Emendamento, anche se non si trattava di un chiaro caso di perquisizione e confisca.

Un ulteriore precedente, forse il più importante, è rappresentato dal caso "*Weeks vs. United States*"[17], che riguardava una condanna per l'utilizzo della posta per il trasporto di biglietti della lotteria. L'imputato fu arrestato da un agente di polizia senza un mandato e, dopo l'arresto , fu perquisita la casa dell'imputato e

[16] "*Boyd vs. United States*", United States Supreme Court, 116 U.S. 616, 1886.
[17] "*Weeks vs. United States*", United States Supreme Court, 232 U.S. 383, 1914.

furono sequestrati numerosi documenti e articoli, nonostante la mancanza di un mandato di perquisizione. Sebbene il convenuto avesse chiesto e ottenuto con successo un ordine del tribunale che disponesse la restituzione della sua proprietà, gli fu negata la restituzione delle prove pertinenti. Venne fatto appello, e la Corte ritenne che tale raccolta di documenti violasse i diritti costituzionali del convenuto e che il tribunale di primo grado non potesse permetterne l'uso al processo.

Il giudice Taft citò diversi altri casi e arrivò alla conclusione che non esistesse un modo ammissibile di applicare la Costituzione americana in questo caso, a meno che non si dimostrasse che il Quarto Emendamento fosse stato inizialmente violato[18]. In questo caso, non vi sarebbe alcuna prova che gli imputati fossero stati in alcun modo obbligati a parlare dai propri telefoni, e si sono impegnati volontariamente in affari. Pertanto, la considerazione della Corte fu limitata al Quarto Emendamento, senza mai oltrepassarlo o metterlo da parte. Taft scrisse nella sua pronuncia che il risultato complessivo del caso Weeks e quelli che ne seguirono fu che il Quarto Emendamento proibì l'introduzione di prove in tribunale se fosse stato ottenuto in violazione del medesimo emendamento. Ciò è in conformità con lo scopo storico del Quarto, in quanto era in parte destinato a impedire l'uso della forza governativa per cercare e sequestrare le proprietà personali e gli effetti personali di un uomo. Taft affermò che: "l'emendamento non proibisce ciò che è stato fatto qui: non c'è stata alcuna ricerca, non c'è stato alcun sequestro, le prove sono state costruite grazie all'uso del senso dell'udito e solo di quello. Non c'era nessuna entrata nelle case o negli uffici degli imputati"[19]. Sottolinea inoltre che si può parlare con un'altra persona a grande distanza via telefono e suggerisce che, poiché i cavi di collegamento non facevano parte né delle case né degli uffici dei coinvolti nel caso Olmstead, non possono essere soggetti alle protezioni del Quarto Emendamento. Lo stesso Taft, in linea con la sua personale filosofia giudiziaria, suggerisce che il Congresso possa

[18] G. Vidal, *La fine della libertà. Verso un nuovo totalitarismo?*, Fazi, 2004.
[19] "*The amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants*".

"naturalmente" estendere tali protezioni alle conversazioni telefoniche passando una legislazione diretta che proibirebbe il loro uso nei processi penali federali. Fino a quando tale legislazione non sarà approvata, tuttavia, "i tribunali non possono adottare tale politica attribuendo un significato ampliato e inusuale al Quarto Emendamento", poiché non vi sono precedenti che consentano a tale emendamento di applicarsi come difesa valida nei casi in cui non c'era stata alcuna ricerca ufficiale e sequestro della persona, dei suoi documenti, effetti materiali tangibili o un'invasione fisica effettiva della proprietà. Conclude che tali intercettazioni come avvenute in questo caso non equivalgono a una ricerca o sequestro nel significato del Quarto Emendamento.

Il processo, dunque, una volta concluso, portò ad un esito negativo per Roy Olmstead, stando ad un'interpretazione letterale del Quarto Emendamento, ma nonostante ciò, fondamentale fu la *dissenting opinion* del giudice supremo Brandeis. Così come quarant'anni prima, diversamente dal collega Warren, egli ribadì quanto alcuni concetti giuridici debbano fare i conti col tempo e con l'evoluzione della società, in modo da evolversi di pari passo e non risultare obsoleti o inefficaci. Egli volle porre l'attenzione sul fatto che una interpretazione così restrittiva del Quarto Emendamento mal si sposava con la necessità di fare i conti con l'evoluzione tecnologica e scientifica del XX secolo, poiché il tempo comporta cambiamenti imprevedibili che solo in una corretta interpretazione delle norme possono trovare una collocazione adeguata. Il discorso continua sottolineando come siano ormai accessibili al governo molti espedienti subdoli e invasivi della *privacy*, e che di certo non erano stati previsti dai fondatori della Costituzione, fin quando ci si attenga ad una interpretazione strettamente letteraria. In conclusione pone un quesito ancora più complesso e specifico: "*Un giorno saranno trovati mezzi grazie ai quali il governo senza rimuovere alcuno scritto da cassetti segreti, potrà riprodurlo in tribunale e con cui gli sarà possibile esporre gli eventi più intimi che possono avvenire in una casa. Può essere che la Costituzione non garantisca alcuna protezione contro una tale invasione della sicurezza dell'individuo?*".

Come è evidente, Brandeis cercava di estrapolare da un caso di specie un problema ben più grave, che era quello di riconoscere come non ci si poteva affidare sempre e comunque ad una semplice interpretazione letterale degli Emendamenti; partendo da questo presupposto egli esorta la Corte Suprema, nella sua qualità di maggiore interprete costituzionale, a non fermarsi alle contingenze di uno stato tecnologico sempre in divenire e a tener conto del vero scopo dei Costituenti, ovvero, nel presente caso, quello di proteggere il diritto ad essere lasciati soli.

Non ci sono dubbi sul fatto che la posizione del giudice Brandeis abbia fornito un assetto completamente nuovo e rivoluzionario sul problema oggetto di studio, eppure, simili argomentazioni non furono sufficienti per essere accolte dalla Corte.

1.1.2 Il Caso "Kats vs. United States" e la *concurring opinion* del giudice Harlan

Un ribaltamento totale rispetto alla causa "*Olmstead vs. United States*" avvenne quarant'anni dopo, nel caso "*Katz vs. United States*"[20], del 1967. La questione fu sempre relativa ad un'intercettazione telefonica operata senza mandato e che si ritenne violare il Quarto Emendamento[21]. Da parte dell'accusa, si riteneva che nonostante l'emendamento suddetto garantisse una tutela contro le perquisizioni e le ricerche senza alcun tipo di mandato, non vi fosse nessun bene tangibile che fosse stato perquisito, e dunque il Quarto Emendamento non poteva

[20] *Charles Katz vs. Unites States*, 389 US 347, 1967.

[21] Nel caso di specie, Katz era sospettato coinvolto in un'attività di gioco d'azzardo a Los Angeles. Tenuto d'occhio da parte della polizia federale, si era notato che faceva spesso uso di una singola cabina telefonica che si ritenne fosse usata per veicolare informazioni derivanti da bische e allibratori. In assenza di mandato, ma senza entrare fisicamente nella cabina, gli agenti introdussero una cimice, posta all'esterno del telefono pubblico. In questo modo vennero registrate diverse conversazioni che permisero di chiedere la condanna di Katz in violazione di una legge federale che vietava il traffico di informazioni illegali sulle scommesse.

essere applicato, poiché la cabina telefonica, trovandosi su un suolo pubblico, era di proprietà pubblica e non costituiva quindi un'area costituzionalmente tutelata. La difesa non potè non richiamare la precedente *dissenting opinion* del caso *Olmstead vs. United States* dell'ormai defunto giudice Brandeis, che, questa volta, risultò decisiva tanto da essere accolta: la Corte si schierò a favore di Katz.

Interessanti furono le posizioni di alcuni giudici favorevoli, in particolar modo Potter Stewart e John Harlan, i quali ritennero che "*quello a cui Katz cercava di sottrarsi non era certo l'occhio indiscreto, ma semmai l'orecchio senza invito*", intendendo come fosse necessario dare una nuova interpretazione al disposto del Quarto Emendamento, affermando che quest'ultimo "*protegge le persone e non i luoghi*". I due proseguirono sostenendo che se la polizia federale avesse richiesto una qualsivoglia autorizzazione prima di procedere, non ci sarebbe stata alcuna violazione nei confronti dell'imputato, mentre nel caso contrario, ovunque un individuo possa trovarsi, egli ha il diritto di sapere che rimarrà immune da ricerche e perquisizioni irragionevoli.

In particolar modo il giudice Stewart, esprimendosi in nome della maggioranza, scrisse: "Uno che occupa (una cabina telefonica), chiude la porta dietro di sé e paga il tributo che gli consente di effettuare una chiamata è sicuramente autorizzato a presumere che le parole che pronuncia nel bocchino non saranno trasmesse al mondo"[22]. Alcuni dettagli, come la chiusura della porta della cabina telefonica, aiutano a determinare se una persona intende partecipare a una conversazione privata. Pertanto, le conversazioni private possono essere effettuate in aree pubbliche. L'opinione della maggioranza redatta del giudice Stewart non contestava il fatto che un magistrato potesse costituzionalmente autorizzare l'intercettazione in questo caso, ma, poiché tale mandato non è stato né cercato né ottenuto, la ricerca è stata pertanto incostituzionale. Allo stesso modo, la Corte disse che non riconosceva alcun diritto generale alla *privacy* nel Quarto

[22] "*One who occupies (a telephone booth), shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world*".

Emendamento: "la protezione del diritto generale alla privacy di una persona, il suo diritto ad essere lasciata in pace da altre persone, è, come la protezione della sua proprietà e della sua stessa vita, lasciata in gran parte alla legge dei singoli Stati"[23].

Infine, il giudice Harlan, nella sua *concurring opinion*, prima riassunse le posizioni della maggioranza e poi propose un test. Le posizioni essenziali della maggioranza erano:

- una cabina telefonica chiusa è un'area in cui, come una casa, e diversamente da un campo, una persona ha una ragionevole aspettativa di *privacy*;
- l'intrusione sia elettronica sia fisica in un luogo privato in questo senso può costituire una violazione del Quarto Emendamento;
- un'invasione di un'area costituzionalmente protetta da parte delle autorità federali è, come la Corte ha da tempo considerato, presumibilmente irragionevole in assenza di un mandato di perquisizione.

Dopodiché il giudice Harlan propose un test a due fasi per riconoscere cosa fosse "privato" per il Quarto Emendamento e che, decisamente, pose le basi per la soluzione di diversi problemi che si sarebbero sviluppati negli anni successivi in materia di diritto alla *privacy*: "*Bisogna chiedersi se esiste un duplice requisito, il primo dei quali è stabilire se la persona ha mostrato un'effettiva e soggettiva aspettativa di privacy, mentre il secondo è che quell'aspettativa sia riconosciuta dalla società come ragionevole*". Nel caso in cui entrambe le aspettative risultino soddisfatte, si potrà ritenere tale diritto alla *privacy* protetto dal Quarto Emendamento.

L'unico parere contrario fu, come anticipato, quello del giudice Hugo Black, il quale sosteneva che il Quarto Emendamento, nel suo complesso, era

[23] "*The protection of a persons's general right to privacy, his right to be let alone by other people, is, like the protection of his property and of his very life, left largely to the law of the individual States*".

inteso unicamente a proteggere "le cose" dalla ricerca fisica e dal sequestro e non era destinato a proteggere la *privacy* personale.

La decisione della Corte nel caso appena analizzato, nonché il testo proposto dal giudice Harlan, hanno fornito spunti che pian piano sono stati immagazzinati nei meccanismi della Suprema Corte e hanno fatto si che il Quarto Emendamento assumesse connotati certamente più moderni. Tutto ciò portò alla necessità di compiere accurate scelte di valori, come un equo bilanciamento tra gli interessi in contrasto, dando anche un significato sostanziale a espressioni come "ragionevole aspettativa di *privacy*" e all'aggettivo "ragionevole" riferito alle perquisizioni e confische da parte degli enti governativi.

Nonostante dal caso *Katz* si fosse registrata una netta evoluzione in tema di *privacy*, dal momento che ci si sganciò completamente dal taglio prettamente "proprietario" fornito dal Quarto Emendamento, si ritenne comunque che la Corte Suprema non avesse recepito sufficientemente e pienamente il diritto alla *privacy* così come suggerito dalla dotta posizione del giudice Harlan, poiché in alcune sue pronunce aveva lasciato prevalere, a discapito proprio del diritto alla *privacy*, altri interessi che avevano un valore solo contingente.

Una posizione così critica nei confronti dell'operato della Corte però non è del tutto condivisibile. L'apporto di essa al tema del diritto alla privacy, successivamente al caso Katz, assieme al supporto sempre presente della dottrina, non può negarsi, seppur con qualche riserva, poiché, senza dubbio, senza di esso non si sarebbero originate le iniziali normative americane in tema di riservatezza[24] che, tutt'oggi, nelle loro forme successive, continuano, in connubio all'operato dell'Unione Europea, a mandare segnali evolutivi al nostro continente.

Inoltre, da ultimo, non si può dimenticare come, grazie all'apporto della Corte, il diritto alla privacy abbia aggiunto alla sua originale caratteristica negativa

[24] Per completezza informativa è giusto ricordare il *FOIA*, *Freedom of Information Act* del 1966, che assicura al cittadino l'accesso a tutte le informazioni sugli enti pubblici tramite un determinato metodo di pubblicità, e il *Privacy Act del 1974*, che integrando il *FOIA* pone una barriera alla circolazione delle informazioni che riguardano il cittadino ed agevola il "diritto di sapere" da parte degli investigati.

(Right to be let alone), una successiva caratteristica positiva, intesa come il diritto della persona di attivarsi al fine di controllare tutte le informazioni che la riguardano e che queste vengano trattate da terzi solo in caso di necessità.

1.1.3 Evoluzione legislativa americana

Questa continua evoluzione del diritto alla *privacy*, partita nel 1890, trova in questi ultimi anni una sua cementificazione nel modello americano, attraverso numerose leggi che hanno coperto vari settori riguardanti i dati personali, dopo le già citate *FOIA* e *Privacy Act*. In particolare vanno ricordate: *HIPAA*[25], *DMCA*[26], *UCITA*[27], *ESIGN*[28], *PATRIOT Act*[29], *FISMA*[30] e *CIPSEA*[31].

1.2 Diffusione della privacy in Europa

Sebbene la ricerca e l'evoluzione del diritto alla privacy nel continente americano sia stata molto impegnativa, di certo l'esperienza del nostro continente

[25] *Health Insurance Portability and Accountability Act*, 1996. La legge consiste in cinque titoli, che disciplinano rispettivamente i lavoratori, le transazioni elettroniche, i conti di spesa medica, i piani di salute di gruppo e le polizze di assicurazione sulla vita.
[26] *U.S. Digital Millennium Copyright Act*, 1998. Tale legge parla solo ed unicamente di copyright.
[27] *U.S. Uniform Computer Information Transactions Act*, 1999. Questo atto è stato un tentativo di redigere un atto uniforme per tutti gli Stati Uniti, ma ognuno era libero o meno di approvarlo, e alla fine fu approvato solo in Virginia ed in Maryland.
[28] *U.S. Congress Electronic Signatures in Global National Commerce Act*, 2000. È una legge approvata dal Congresso degli Stati Uniti per facilitare l'uso dei registri elettronici e firme elettroniche, garantendo la validità e l'effetto giuridico dei contratti stipulati per via elettronica.
[29] *U.S. Provide Appropriate Tools Required to Intercept and Obstruct Terrorism*, 2001. L'atto in questione consente all'FBI di effettuare ricerche di qualsivoglia tipo, anche nei registri delle imprese o registri bibliotecari e finanziari, senza un ordine del tribunale.
[30] *Federal Information Security Management Act*, 2002. Con questo atto si impone a ciascuna agenzia federale di sviluppare, documentare e attuare un programma a livello di agenzia per fornire sicurezza alle loro informazioni.
[31] *Confidential Information Protection and Statistical Efficiency Act*, 2002. La legge stabilisce tutele uniformi di riresvatezza.

non è stata da meno. A differenza della Corte Suprema statunitense, che ha fatto da elemento unificatore, in Europa questo elemento è mancato, poiché hanno pesato molto le numerose differenze tra i vari sistemi giuridici di tradizione romanistica. Sicuramente un grande apporto in materia è stato fornito dall'Italia, nonostante un primo accenno in merito si sia avuto in area germanica. In particolar modo un primo approccio ai diritti dell'individuo si è avuto in Germania dopo l'entrata in vigore del *BGB*[32], e in Svizzera, dove tali diritti della personalità ebbero legittimazione e protezione per la prima volta, grazie all'entrata in vigore del *ZGB*[33].

Presto il dibattito sul riconoscimento giuridico dei diritti della personalità raggiunse anche gli stati confinanti, fra cui la Francia. Uno dei più importanti riferimenti dottrinali che si ricordano fu quello di Alphonse Boistel, il quale, basandosi principalmente sul diritto d'autore, elabora la nozione di *droit moral*, la quale in poco tempo trovò collocazione nel sistema giuridico francese. Nel 1909 nasce la categoria dei diritti della personalità, supportata soprattutto dal giurista francese Perreau, il quale sviluppa la sua posizione basandosi sulla norma di chiusura del *Code Civil*[34] presente nell'articolo 1382: "*Ogni atto commesso da un uomo danneggiando un altro, obbliga chi ha causato il danno a risarcire*"[35]. Partendo da questo presupposto, non siamo di fronte ad una tutela diretta, bensì, in ragione del fatto che la norma sopracitata è una norma aperta, l'Autore rintraccia e giustifica la necessità di una protezione della vita privata, per cui, a fronte di un pregiudizio o di un danno ingiusto, il giudice dovrà comminare una sanzione risarcitoria.

È tuttavia evidente come, in seguito a quanto appena riportato, si sia ancora piuttosto lontani da una sufficiente tutela dei diritti della personalità e, di

[32] Il *Bürgeeliches Gesetzbuch*, abbreviato con la sigla *BGB*, è il codice civile tedesco, che entrò in vigore il 1 gennaio del 1900.
[33] Il *Zivil Gedetzbuch*, abbreviato con la sigla *ZGB*, è il codice civile svizzero, entrato in vigore nel 1912.
[34] Il *Code Civil*, o *Code Napoleon*, è il primo codice civile francese, entrato in vigore nel 1804.
[35] "*Tout fait quelconque de l'homme, qui cause un dommage à autrui, oblige celui par la faute duquel il est arrivé, à le réparer*"

conseguenza, di un diritto alla riservatezza. Il passo successivo, come vedremo a breve, avvenne proprio in Italia, per mano di Adolfo Ravà, il quale effettuò un'interessante analisi intrecciando filosofia e diritto per individuare la personalità dal punto di vista giuridico intesa come "diritto sulla propria persona".

1.3 Primi studi e teorie sul concetto di privacy in Italia

Gli studi filosofici e giuridici compiuti da Alfonso Ravà agli inizi del XX secolo rappresentarono un input importante a quelli che poi furono gli innumerevoli dibattiti in tema di diritti della personalità e, in particolare, sul diritto alla riservatezza. Non essendovi espliciti riconoscimenti del diritto alla riservatezza, Ravà provò a rinvenire la sua giustificazione da norme dell'ordinamento che in qualche modo potevano esserne una manifestazione. Egli intuì che "*la qualità di persona richiede ed esige che alla persona stessa sia riservata una certa sfera relativa ai dati più gelosi e più intimi di essa e della sua attività*"[36], e da ciò, secondo lui, scaturisce un generale diritto alla riservatezza. Per giustificare l'osservazione appena citata, l'autore richiama varie norme del nostro ordinamento, quali l'art. 10[37] del Codice Civile del 1942 e soprattutto gli artt. 96 e 97[38] della legge sul Diritto d'Autore del 22 aprile 1941, n.633. Il diritto alla riservatezza si sarebbe dovuto ricavare da queste norme in virtù di un

[36] Alfonso Ravà, *Istituzioni di diritto privato*, Cedam, Padova, 1938.
[37] "Qualora l'immagine di una persona o dei genitori, del coniuge o dei figli sia stata esposta o pubblicata fuori dai casi in cui l'esposizione o la pubblicazione è dalla legge consentita, ovvero con pregiudizio al decoro o alla reputazione della persona stessa o detti congiunti, l'autorità giudiziaria, su richiesta dell'interessato, può disporre che cessi l'abuso, salvo il risarcimento dei danni".
[38] Art. 96: "Il ritratto di una persona non può essere esposto, riprodotto o messo in commercio senza il consenso di questa, salve le disposizioni dell'articolo seguente". Art. 97: "Non occorre il consenso della persona ritrattata quando la riproduzione dell'immagine è giustificata dalla notorietà o dall'ufficio pubblico coperto, da necessità di giustizia o di polizia, da scopi scientifici o didattici o culturali, o quando la riproduzione è collegata a fatti, avvenimenti, cerimonie di interesse pubblico o svoltosi in pubblico. Il ritratto non può tuttavia essere esposto o messo in commercio, quando l'esposizione o la messa in commercio rechi pregiudizio all'onore, alla reputazione od anche al decoro della persona ritratta".

procedimento analogico, aventi entrambi la stessa *ratio*, in particolar modo nella parte relativa all'immagine. Alla base di questa tesi dell'autore vi è l'art. 12, comma 2[39], delle disposizioni sulla legge in generale[40]. L'articolo appena preso in considerazione, oltre ai casi di *analogia legis*, prevede anche la possibilità di *analogia iuris*, ovvero un'interpretazione che si basa sul ricorso ai principi generali dell'ordinamento giuridico dello Stato. Così facendo Ravà afferma la rilevanza assoluta degli attributi fondamentali della personalità e la necessità di una loro considerazione indipendentemente da una espressa manifestazione di volontà da parte del legislatore. Conclude quindi includendo nel novero dei diritti della personalità anche il diritto alla riservatezza, rintracciando in questo modo l'esistenza di un principio generale a tutela della stessa.

Su una posizione completamente opposta si pone la dottrina del Pugliese[41], il quale ritiene come, in realtà, queste norme siano poste a protezione di un bene superiore al singolo individuo, che sarebbe la personalità stessa della persona. Egli afferma che non esiste alcuna norma che riconosca esplicitamente il diritto alla riservatezza e che non si possa neanche raggiungere attraverso un'interpretazione analogica delle disposizioni giuridiche prese in considerazione precedentemente da Ravà, poiché, ai sensi dell'art. 14[42] delle disposizioni sulla legge in generale, farebbero eccezione alle regole generali per le quali vige il divieto di analogia.

Oltre al dibattito sull'esistenza dei diritti della personalità, si instaurò un ulteriore dibattito sulla loro eventuale unicità o molteplicità. Un primo orientamento affermava l'esistenza di un unico diritto della personalità, secondo la posizione monista, la quale vedeva la persona umana come valore unitario. Ma nonostante alcuni vantaggi che una simile opinione, soprattutto per la sua possibile

[39] "Se una controversia non può essere decisa con una precisa disposizione, si ha riguardo alle disposizioni che regolano casi simili o materie analoghe; se il caso rimane ancora dubbio, si decide secondo i principi generali dell'ordinamento giuridico dello Stato".
[40] Sono dette anche "preleggi" e sono collocate all'inizio del codice civile, anteriormente agli articoli dello stesso, e sono un gruppo di 16 articoli.
[41] G. Pugliese, *Il preteso diritto alla riservatezza e le indiscrezioni cinematografiche*, Zanichelli, Bologna, 1954.
[42] "Le leggi penali e quelle che fanno eccezione a regole generali o ad altre leggi non si applicano oltre i casi e i tempi in esse considerati".

elasticità, poteva portare all'interno dell'ordinamento, questa non fu esente da critiche, in particolar modo da De Cupis[43], il quale supporta invece la posizione pluralista dei diritti della personalità. Egli giustificava la sua posizione delineando la persona umana come una molteplicità di aspetti e interessi, ognuno con sue peculiari caratteristiche.

1.3.1 Apporti giurisprudenziali in tema di diritto alla riservatezza

Importante in questo scenario è stata l'evoluzione giurisprudenziale della Corte di Cassazione sul tema oggetto di analisi. I primi casi, negli anni '50, provenivano da una giurisprudenza di merito che affrontò diversi casi sviluppatisi da opere cinematografiche e pubblicazioni relative a vicende personali di personaggi noti. L'orientamento della Corte era che "*nessuna disposizione di legge autorizza a ritenere sancito come principio generale il rispetto assoluto dell'intimità della vita privata salvo che l'operato dell'agente, offendendo, ricada nello schema generale del fatto illecito*". Dunque, la soluzione poteva essere trovata nel principio del *neminem laedere* dell'art. 2043[44] del Codice Civile, senza la necessità di sviluppare nuovi istituti. Lo scenario cambiò fortemente con la sentenza n. 990 del 1963 della Corte di Cassazione, nella cui massima si legge: "*Sebbene non sia ammissibile il diritto tipico alla riservatezza, viola il diritto assoluto di personalità, inteso quale diritto erga omnes alla libertà di autodeterminazione nello svolgimento della personalità dell'uomo come singolo, la divulgazione di notizie relative alla vita privata, in assenza di un consenso almeno implicito, ed ove non sussista, per la natura dell'attività svolta dalla persona e del fatto divulgato, un preminente interesse pubblico di conoscenza*". Nonostante manchi un diritto tipico alla riservatezza, viene riconosciuto un diritto

[43] A. De Cupis, *I diritti della personalità*, Giuffrè Editore, Milano, 1982.
[44] "Qualunque fatto doloso o colposo, che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno".

unitario assoluto della personalità, secondo la posizione monista, ma il risultato fu per la dottrina ancora insoddisfacente.

La situazione rimase incerta sino al 1975, anno in cui vi fu una svolta definitiva, con un'ulteriore sentenza della Cassazione[45] che affermò definitivamente l'esistenza di un diritto alla riservatezza. A seguito dell'analisi del caso di specie[46], la Corte rilevò un duplice fondamento, implicito ed esplicito, del diritto alla riservatezza. Il primo venne individuato "*in quel complesso di norme ordinarie e costituzionali che, tutelando aspetti peculiari della persona, nel sistema dell'ordinamento sostanziale, non possono non riferirsi anche alla sfera privata di essa*[47]", mentre il secondo "*in tutte quelle norme, contenute in modo particolare in leggi speciali, nelle quali si richiama espressamente la vita privata del soggetto o addirittura la riservatezza*".

La Corte riuscì a questo punto a sviluppare in maniera definitiva l'articolo 2[48] della Costituzione, alla luce del diritto in questione. Essa afferma che nell'articolo 2 è presente anche e finalmente il diritto alla riservatezza. Infatti, dal momento che la Repubblica garantisce i diritti inviolabili dell'uomo nei quali è assolutamente imprescindibile quello della personalità, allo stesso modo lo è il diritto alla riservatezza, definito dalla Corte come "*il diritto che consiste nella tutela di quelle situazioni e vicende strettamente personali e familiari, le quali, anche se verificatesi fuori del domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile contro le ingerenze che, sia pur compiute con*

[45] Cassazione Civile, 27 maggio 1975, n. 2129.
[46] L'episodio è relativo a personaggi di pubblico interesse: Soraya Esfandiari, seconda moglie di Mohammad Reza Pahlavi, ultimo Scià di Persia, era stata fotografata in compagnia di un uomo in atteggiamenti intimi all'interno della sua abitazione, e queste foto erano state pubblicate da alcune delle principali testate giornalistiche nazionali contro le quali la donna intentò causa.
[47] La Corte cita in particolar modo: diritto al corpo (art. 5 c.c.), al nome (artt. 6-9 c.c.), all'immagine (art. 10 c.c.), all'anonimato e all'inedito (artt. 21 e 24 legge diritto d'Autore), all'onore contro la rivelazione di fatti determinati (art. 595, secondo comma, c.p.), al domicilio (art. 614 c.p.), alla corrispondenza (artt. 616 c.p. e 48 legge fall.).
[48] "La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale".

mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione e il decoro, non siano giustificate da interessi pubblici preminenti".

Per giungere ad una definizione di questo tipo, però, la Corte dovette fare chiarezza dal punto di vista lessicale, poiché con l'espressione "diritto alla riservatezza" sono indicate diverse ipotesi, che si possono sintetizzare in tre aspetti.

La prima si ricollega al concetto ed alla tutela del domicilio secondo il "*right to be let alone*" anglosassone. Nella seconda, la Corte invece è fin troppo generica, facendo riferimento al "riserbo della vita privata" da qualsiasi ingerenza o la "*privacy*", concetti troppo vasti ed indeterminati. La Corte accoglie la posizione intermedia, la terza, che riporta in limiti ragionevoli la portata di questo diritto e che può identificarsi nelle formule che fanno riferimento ad una certa sfera della vita individuale e familiare, alla illesa intimità personale in certe manifestazioni della vita di relazione, a tutte quelle vicende, cioè, il cui carattere intimo è dato dal fatto che esse si svolgono in un domicilio ideale, non materialmente legato ai tradizionali rifugi della persona umana. La Corte così facendo fa convogliare tutti i passati orientamenti in uno unico e solido, e richiama anche altri articoli della Costituzione[49] e vari spunti di natura internazionale[50], a sostegno della sua posizione.

[49] Sono richiamati: l'art. 3 dal punto di vista dell'eguaglianza sostanziale, l'art. 13 circa l'inviolabilità della libertà personale, gli artt. 14 e 15 per l'inviolabilità di domicilio, della libertà e della corrispondenza, l'art. 27 dal quale dovrebbero trarsi dei limiti alla diffusione di notizie riguardanti vicende dell'imputato e sui cd. "retroscena" dei delitti, l'art. 29 comma 2 che riconosce il carattere originario e l'inviolabile autonomia della famiglia e l'art. 41 laddove l'iniziativa economica trova un limite nel rispetto della libertà e della dignità umana.

[50] Viene citata la " Dichiarazione universale sui diritti dell'uomo" (approvata nel 1948 dall'ONU), ed il "Patto internazionale relativo ai diritti civili e politici" (approvato dall'ONU nel 1966). Inoltre si fa anche riferimento alla Convenzione Europea sui Diritti dell'Uomo (CEDU, firmata a Roma il 4 novembre del 1950), in particolare al suo articolo 8, il quale recita testualmente: "Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui".

La lunga attesa prima della tipizzazione del diritto alla riservatezza a posteriori si è rivelata positiva, poiché si sono potuti sfruttare tanti appigli di stampo nazionale ma soprattutto tanti di origine sovranazionale. Questa sentenza tuttavia è solo l'inizio in materia di riservatezza e *privacy*, e sarà considerata come lo snodo fondamentale che avrebbe giustificato future leggi in materia.

1.3.2 Direttiva 95/46/CE e legge n. 675 del 1996

Così come in Italia, anche nel resto d'Europa la seconda metà del XX secolo fu fortemente caratterizzata da un'evoluzione giuridica in tema di diritto alla riservatezza. Il primo provvedimento europeo fu la Convenzione di Strasburgo del 28 gennaio 1981 n. 108[51] che approfondiva l'articolo 8 della CEDU. La Convenzione enuncia il suo scopo all'articolo 1: "garantire, sul territorio di ogni nazione aderente, ad ogni persona fisica, qualunque siano la sua cittadinanza o residenza, il rispetto dei diritti e delle libertà fondamentali, ed in particolare del diritto alla vita privata, nei confronti dell'elaborazione automatizzata dei dati di carattere personale che la riguardano (protezione dei dati)".

Nel diritto alla riservatezza così inteso comincia a prendere piede in modo sempre più evidente la componente positiva rientrante nella tutela e protezione dei dati personali, che trova una sua definitiva regolamentazione, in maniera anche molto dettagliata, nella direttiva 95/46/CE[52]. Essa si instaura su un concetto cardine che sarebbe stato il fondamento di ogni normativa nazionale: i sistemi di trattamento dei dati sono al servizio dell'uomo indipendentemente dalla sua nazionalità o residenza, e ne debbono rispettare le libertà e i diritti fondamentali, in particolare la vita privata. In questo modo la direttiva è stata costruita al fine di

[51] Recepita in Italia con legge 21 febbraio 1989, n. 98.
[52] Direttiva del Parlamento Europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

proteggere i diritti e le libertà della persona in ordine al trattamento dei dati personali stabilendo i principi relativi alla legittimazione del trattamento dei dati.

In Italia, il recepimento di questa direttiva fu quasi immediato ed avvenne con la legge del 31 dicembre 1996 n. 675[53]. Inizialmente l'opinione pubblica italiana accettò questa legge con qualche riserva, poiché sentenze precedenti avevano delineato il diritto alla *privacy* come un diritto elitario spettante a poche persone privilegiate che erano sotto gli occhi dei riflettori e reclamavano il loro diritto d'esser lasciate in pace, un po' come avvenne in America, dove un simile diritto non era considerato proprio del cittadino comune. La legge 675/96, però, cambia completamente le carte in tavola, recependo perfettamente le indicazioni comunitarie e normativizzando il problema del trattamento dei dati personali nell'era dell'informatica, riuscendo a tutelare in questo modo la totalità dei cittadini. Da tale direttiva è stata istituita la figura del "Garante per la protezione dei dati personali"[54]. Il Garante è un organo collegiale che riveste un ruolo fondamentale poiché, sotto un certo punto di vista, personifica gran parte dei principi precedentemente esaminati e analizzati. I particolare i suoi compiti sono:

- Controllare che i trattamenti siano effettuati nel rispetto delle norme di legge
- Ricevere ed esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati dagli interessati
- Vietare, anche d'ufficio, i trattamenti illeciti o non corretti ed eventualmente disporne il blocco
- Promuovere la sottoscrizione di codici di deontologia e buona condotta di determinati settori

[53] Legge n. 675 del 31 dicembre 1996, "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali".
[54] Istituito con l'articolo 30 della suddetta legge, tale organo è costituito da quattro membri, che sono eletti metà dalla Camera dei Deputati e metà dal Senato. Successivamente i componenti eleggono nel loro ambito un presidente, il cui voto prevale in caso di parità. Adesso è in carica Antonello Soro, che ha succeduto a Stefano Rodotà e Francesco Pizzetti.

- Segnalare al Governo e al Parlamento l'opportunità di provvedimenti normativi richiesti dall'evoluzione del settore
- Esprimere pareri nei casi previsti
- Curare la conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità e in materia di misure di sicurezza dei dati
- Denunciare i fatti configurabili come reati perseguibili d'ufficio conosciuti nell'esercizio delle sue funzioni
- Tenere il registro dei trattamenti
- Predisporre una relazione annuale sull'attività svolta da presentare al Governo e al Parlamento
- Essere consultato da Governo o Ministri quando questi predispongono norme che incidono sulla materia
- Cooperare con le altre autorità amministrative indipendenti
- Organizzare il proprio ufficio ed il proprio organico ed il loro trattamento giuridico, economico ed amministrativo

Per completezza sul Garante va aggiunto che è in suo potere anche disporre sanzioni amministrative o penali nei casi previsti dalla legge.

Il legislatore, andando oltre quelle che erano le aspettative comunitarie, apporta alcune importanti aggiunte rispetto alla direttiva, come il rispetto della dignità personale oltre che dei diritti e delle libertà fondamentali, e la tutela dell'identità personale oltre che della riservatezza. Tale legge, perciò, ha avuto una duplice funzione, in quanto ha positivizzato le figure giurisprudenziali del diritto alla riservatezza ed all'identità personale e inoltre ha definitivamente sancito l'importanza, tramite il richiamo alle libertà e diritti fondamentali di dignità della persona, degli sforzi dottrinali e giurisprudenziali susseguitisi nel tempo. In questo modo, come profetizzato dal giudice Brandeis, essa ha definitivamente messo in chiaro il fatto che il diritto alla *privacy* altro non è che una porzione di qualcosa di

molto più grande, poiché a fronte di un'evoluzione tecnologica esponenziale, crescono in maniera altrettanto esponenziali le possibilità che una violazione del diritto alla riservatezza diventi possibile. La legge in questo modo abbandona definitivamente la sola concezione negativa del diritto ad essere lasciati soli e ne estende l'operatività alla porzione positiva, regolando il controllo attivo dei dati personali e rendendolo proporzionale alle moderne necessità di pubblicità e informazione.

In definitiva, si può dire quindi raggiunto un diritto alla *privacy* polifunzionale, il quale offre una tutela completa alla persona.

1.3.3 Direttiva 2002/58/CE e Codice Della Privacy (D.lgs n. 196/2003)

Il "Codice della Privacy", emanato il 30 giugno 2003 col D.lgs. n. 196, rappresenta la conclusione del percorso storico alla ricerca del concetto di *privacy*. Ci sono dei motivi di facile comprensione per cui il legislatore, a soli sei anni di distanza, ha emanato una nuova normativa in materia: subito dopo la legge del 1996, furono emanati una serie di decreti legislativi, decreti del Presidente della Repubblica e regolamenti vari di accompagnamento che trasformarono la legislazione sulla *privacy* in una "giungla giuridica". In più, poco prima era stata emanata la direttiva 2002/58/CE, relativa alla vita privata e alle comunicazioni elettroniche, la quale necessitava di un recepimento nel panorama nazionale.

Il Codice della Privacy non ha apportato alcun tipo di cambiamento agli elementi fondamentali della disciplina previgente, bensì si prefissava di fornire una disciplina più approfondita e soprattutto unitaria, così da superare il "caos legislativo" presente sino a quel momento. Inoltre, siccome il codice presente sottolinea fortemente la presenza di un diritto alla protezione dei dati personali, all'interno del più vasto diritto alla riservatezza, bisogna ricordare come questo

diritto abbia ricevuto un riconoscimento comunitario all'articolo 8[55] della Carta dei Diritti Fondamentali dell'Unione Europea, firmata a Nizza il 7 dicembre del 2000. Dal punto di vista comunitario, non manca un riferimento anche al più generale e vasto concetto di riservatezza, contenuto per l'appunto proprio nell'articolo precedente (art. 7)[56].

Dal punto di vista strutturale, il codice è strutturato in tre parti e tre allegati[57]:

- Articoli 1-45 → Disposizioni generali relativi alle regole fondamentali della disciplina del trattamento dei dati personali
- Articoli 46-140 → Disposizioni particolari per specifici trattamenti ad integrazione o eccezione delle disposizioni generali della prima parte
- Articoli 141-186 → Disposizioni relative alle azioni di tutela dell'interessato e al sistema sanzionatorio

Il codice prevede che all'interessato, ovvero colui al quale i dati si riferiscono, vada garantito il diritto di accesso a tutte le informazioni sulla propria persona, detenute e trattate da terzi. Infatti, all'articolo 7 è prevista la possibilità di conoscere l'autore del trattamento e in più come e a che fine avviene il trattamento e in soggetti a cui tali dati possono essere ceduti (previo consenso informato). L'interessato ha la facoltà di verificare che i dati siano veritieri in virtù del suo diritto di accesso, e può inoltre richiedere l'aggiornamento o, qualora ritenga che gli stessi siano trattati in maniera difforme dalla legge, può chiederne la

[55] Tale articolo, rubricato "protezione dei dati di carattere personale", prevede che "ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 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 individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".

[56] L'articolo 7, rubricato "rispetto della vita privata e della vita familiare", prevede che "ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni".

[57] Allegato A, relativo ai codici di condotta; allegato B, concernente il disciplinare tecnico in materia di misure minime di sicurezza; allegato C, sui trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia.

cancellazione o il blocco. Successivamente, se si riscontra una lesione nei diritti sui propri dati, come ad esempio la raccolta senza consenso o il consenso acquisito senza aver fornito l'informativa di legge, si può ricorrere al Garante per la protezione dei dati personali. Nei casi più gravi, il bene giuridico in questione può essere supportato anche da una tutela penale grazie ad un apposito apparato sanzionatorio.

Infine, un ultimo appunto va riferito al titolo del decreto in questione: sebbene in Gazzetta Ufficiale sia stato pubblicato col titolo "Codice in materia di protezione dei dati personali", la dicitura comunemente utilizzata è quella di Codice o Legge della Privacy. Purtroppo tale dicitura, seppur appoggiata dal primo Garante Stefano Rodotà, non è dal punto di vista giuridico totalmente soddisfacente, poiché non riesce a far risaltare quelle che sono le finalità reali ed ermeneutiche della normativa, cioè garantire che il trattamento dei dati personali avvenga all'interno di limiti prestabiliti e non di difendere la sfera complessiva del diritto alla riservatezza del cittadino.

In un certo senso, aderire alla seconda definizione significherebbe riconoscere nel codice più una carta sul diritto alla riservatezza, con una sorta di connotato negativo, piuttosto che una legge dalle ripercussioni che derivano dal trattamento dei "dati personali" dell'individuo, i quali si pongono, in modo attivo, come conseguenti ripercussioni di un diritto alla *privacy*[58].

1.4 Riflessioni

Possiamo concludere l'analisi sulla nascita del concetto di privacy ripercorrendo un po' i caratteri principali della sua evoluzione. Inizialmente la privacy consisteva in un concetto che semplicemente separava la vita pubblica dalla vita privata, ed ha visto la sua massima estensione nel principio di "right to

[58] F. Di Resta, *Le recenti modifiche al Codice della Privacy*: note critiche, Altalex, 2012.

be let alone" di stampo americano, anche se veniva visto come un diritto appartenente solo alla classe borghese e non alla portata di tutti i cittadini. Nel panorama americano il concetto di riservatezza ha assunto la fisionomia, dunque, di "diritto ad essere lasciati soli", e, di conseguenza, diritto a non subire ingerenze o invasioni dall'esterno. Tale estensione del concetto però aveva una valenza prettamente negativa, poiché rappresentava una "libertà da" e non una "libertà di" da parte dei cittadini. Grazie a numerosi studi e numerose sentenze, di cui alcune fondamentali sopracitate, però, il diritto alla riservatezza ha trovato un riferimento prima in Costituzione americana, dopodiché è stato disciplinato in numerose leggi, facendo in modo che fosse accessibile e fruibile da parte di ogni cittadino. Inoltre si è aggiunta alla sua originaria connotazione negativa, una connotazione anche positiva: il diritto della persona di attivarsi per essere a conoscenza e proteggere tutti i suoi dati che siano in possesso di terzi.

Dall'esperienza americana si è sviluppato un filone normativo che ha portato anche in Europa e, di conseguenza, in Italia, lo sviluppo di questo diritto, che lo vede definitivamente affermato sul duplice binario della riservatezza e della protezione dei dati. E questo è il traguardo finale raggiunto dalla normativa odierna: parlare di privacy e di protezione dei dati non è la stessa cosa. Privacy è il diritto di scegliere cosa, del nostro spazio personale, vogliamo rendere conoscibile agli altri; il diritto alla protezione dei dati consiste invece nella protezione di quei dati che noi volontariamente abbiamo affidato al trattamento esterno da parte di terzi.

CAPITOLO 2

IL GDPR (GENERAL DATA PROTECTION REGULATION)

Il GDPR (General Data Protection Regulation)

Il 4 maggio 2016 è stato pubblicato sulla Gazzetta ufficiale dell'Unione europea il Regolamento dell'Unione Europea n. 679, il Regolamento generale sulla protezione dei dati (GDPR[59]) sulla protezione dei dati personali e la libera circolazione dei dati personali. Il Regolamento è entrato pienamente in vigore a decorrere dal 25 maggio 2018, data dalla quale risulta abrogata la direttiva 95/46/CE[60].

Il nuovo Regolamento europeo apre uno scenario innovativo nella disciplina della materia poiché, seppur le fondamenta della *privacy* risultano confermate, sono stati puntualizzati molteplici aspetti, sono state specificate le modalità di attuazione di taluni adempimenti, sono state significativamente inasprite le sanzioni, nonché introdotte una serie rilevante di novità. Il Regolamento reca anche alcuni rilevanti mutamenti nelle scelte di politica del diritto.

2.1 Caratteristiche generali del Regolamento UE 2016/679

Il GDPR nasce, come ampiamente illustrato nei considerando[61] del testo, dalla constatazione della frammentazione della disciplina sulla protezione dei dati personali nell'Unione Europea e dalla rilevazione della diffusa incertezza giuridica concernente l'applicazione della normativa. L'esigenza è stata quella di assicurare un'applicazione omogenea della normativa vigente.

[59] "*General Data Protection Regulation*", GDPR, Regolamento UE n. 2016/679, del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
[60] Dal 25 maggio 2018 la Direttiva 95/46/CE (regolamento generale sulla protezione dei dati) è stata abrogata.
[61] Sono ben 173 i "considerando" anteposti al testo del Regolamento.

Trattandosi di un Regolamento, esso è direttamente applicabile in tutti gli Stati membri dell'UE, senza la necessità di atti di recepimento nei singoli Stati nazionali. Non si tratta dunque di uno strumento di armonizzazione, bensì di uno strumento di uniformazione del diritto per gli Stati europei, eliminando così in radice quelle piccole differenze che rendono difficile realizzare compiutamente un mercato unico.

Come si vedrà più avanti in questa trattazione, a livello nazionale italiano rimane in vigore una normativa specifica in materia di *privacy*, il Codice della Privacy, rappresentato dal D.Lgs. 196/2003; il codice appena citato è stato adattato alle disposizioni presenti nel nuovo Regolamento 679/2016 da un atto di recente emanazione, il D.Lgs. 101/2018, entrato in vigore il 19 settembre 2018.

Il Regolamento UE 2016/679 raccoglie l'esperienza maturata in Europa negli ultimi vent'anni e dunque, quasi come fosse un Testo Unico, cerca di riordinare e razionalizzare il sistema, ed è in questo senso che vanno lette alcune disposizioni il cui contenuto, pur non essendo innovativo, arricchisce e rende aggiornata la normativa. Ci si riferisce a concetti quali la definizione di dato personale, la disciplina del consenso e altri. Alcune definizioni sono invece nuove, come quella sui dati biometrici e quella sulle tecniche di pseudonimizzazione. In altre, sono state aggiunte delle precisazioni, come nel caso dell'informativa. Inoltre, è stato inserito un articolo ad hoc sul consenso dei minori e sono stati poi dettagliatamente disciplinati alcuni diritti, come il diritto alla cancellazione dei dati, già noto come "diritto all'oblio". È stato introdotto il diritto alla portabilità dei dati e una disciplina sul trasferimento dei dati all'estero, unitamente ad alcuni meccanismi per garantire un'applicazione uniforme del Regolamento nell'Unione. Mutano infine le disposizioni sul foro competente e il regime di responsabilità civile.

2.2 Capo I: disposizioni generali

Non si può che cominciare l'analisi del presente testo dalla sua prima disposizione. L'articolo 1, rubricato "oggetto e finalità", che recita:

1. *Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.*
2. *Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.*
3. *La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.*

La disposizione in esame, il cui testo è praticamente identico a quello contenuto nella Proposta originaria della Commissione, presenta alcune analogie con la Direttiva 95/46/CE, ma anche una grande differenza. Le analogie sono rappresentate:

- dall'individuazione di un duplice obiettivo, ovvero "la protezione delle persone fisiche con riguardo al trattamento dei dati personali" e "la libera circolazione di tali dati";
- dalla formulazione del secondo di questi obiettivi: l'articolo 1 paragrafo 3 del Regolamento è molto simile all'articolo 1[62] della Direttiva.

La grande differenza, che riguarda il primo dei due obiettivi, si trova invece nel paragrafo 2, e consiste nell'espressione "in particolare il diritto alla

[62] Articolo 1 Direttiva 95/46/CE: "1) Gli stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali. 2) Gli Stati membri non possono restringere o vietare la libera circolazione dei dati personali tra Stati membri, per motivi connessi alla tutela garantita a norma del paragrafo 1".

protezione dei dati personali", utilizzata anche nel Preambolo del Regolamento, precisamente nei Considerando 2, 9 e 166.

Se osserviamo attentamente, in vari documenti (Direttiva 95/46/CE, Direttiva 97/66/CE, Regolamento CE n. 45/2001, Direttiva 2002/58/CE e la Decisione quadro 2008/977/GAI) troviamo sempre la stessa formula in base alla quale la protezione dei dati personali è funzionale alla tutela, in generale, dei diritti e delle libertà fondamentali, ma in particolare del diritto alla vita "privata/*privacy*". La formula in questione è ripresa dall'articolo 1[63] della Convenzione di Strasburgo 108 del 1981: "*Scopo della presente Convenzione è quello di garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano ("protezione dei dati")*".

Possiamo dunque estrapolare da tale disposizione uno schema che prevede:

- un *quid* chiamato "*data protection*";
- un collegamento fra tale "*data protection*" e la tutela, in generale, dei diritti e delle libertà fondamentali;
- un collegamento speciale fra tale "*data protection*" e la tutela del diritto alla "*privacy*".

Ritornando dunque all'articolo 1 del Regolamento 2016/679, si può osservare come esso mantenga lo schema appena estrapolato e i suoi primi due elementi, ma non il terzo: in luogo del diritto alla "vita privata/*privacy*" troviamo il "diritto alla protezione dei dati personali/*right to the protection of personal*

[63] "*The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")*".

data". Il secondo diritto non si aggiunge al primo e non è neanche una sua componente, bensì semplicemente lo sostituisce. Nel Regolamento il diritto alla vita privata viene totalmente sostituito dal diritto alla protezione dei dati personali.

Perché sostituire il binomio "*privacy*/vita privata" col diritto alla protezione dei dati personali? Quest'ultimo è formato da sei componenti essenziali:

1. il requisito del "principio di lealtà" nel trattamento dei dati ("*fair processing*");
2. il requisito del trattamento "per finalità determinate" ("*for specified purposes*");
3. il requisito del "fondamento legittimo" ("*legitimate basis*"), che può essere "previsto dalla legge" ("*laid down by law*"), oppure più semplicemente può essere il "consenso della persona interessata" ("*consent of the person concerned*");
4. il diritto di accesso ai dati ("*right of access to data*");
5. il diritto di ottenere la loro rettifica ("*right to have it rectified*");
6. il controllo da parte di un soggetto indipendente.

Anche se questi elementi sono ripresi da strumenti giuridici in materia di *privacy*, sarebbe un errore parlare del diritto alla protezione dei dati personali come se discendesse dal diritto alla *privacy*. Il diritto alla protezione dei dati personali è a tutti gli effetti un diritto autonomo, e si colloca su un piano diverso, per capire il quale è opportuno partire proprio da una delle sei componenti precedentemente ricordate: il diritto di accesso ai dati. Il diritto in questione, infatti, da molti punti di vista risulta avere un legame molto più stretto con il diritto di accesso ai documenti pubblici, che con lo stesso diritto alla *privacy*. Il diritto alla protezione dei dati personali può essere considerato come la versione europea di quel diritto fondamentale che, in numerosi Stati, soprattutto dell'America Latina, viene denominato "*habeas data*". Con tale dicitura si intende "abbi il controllo dei tuoi dati", e può essere infatti definito come il diritto degli individui di chiedere

l'accesso agli archivi che contengono informazioni su di loro, e di rettificare i dati inesatti[64]. L'idea di fondo è quella di non limitarsi a proteggere i dati dalle ingerenze esterne, ma permettere alla persona interessata di avere un controllo effettivo su tali dati.

In definitiva, il diritto alla protezione dei dati personali non si limita ad escludere l'interferenza altrui e ad offrire una tutela statica, negativa, ma, al contrario, si concretizza in poteri di controllo e di intervento, e siamo di fronte ad una tutela dinamica, che segue i dati nella loro circolazione. Un simile approccio ha naturalmente ricadute molto significativa sugli istituti disciplinati dal Regolamento 2016/679, poiché alcune delle novità più significative sono figlie di questo diverso tipo di tutela. Inoltre, la tutela non viene più garantita esclusivamente ai dati che, in un modo o nell'altro, possono essere considerati come dati relativi alla vita privata, ma ai dati personali in quanto tali. Siamo dunque di fronte ad una tutela non parziale, ma piena, dei dati personali[65].

Ultimata l'analisi dell'articolo iniziale del Regolamento, bisogna focalizzarsi sull'ambito di applicazione. L'ambito di applicazione materiale resta pressoché invariato rispetto al passato: l'articolo 2 paragrafo 1 del Regolamento, infatti, recita "*il presente 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*", e risulta perciò corrispondente al "vecchio" articolo 3 paragrafo 1 della Direttiva 95/46/CE.

Anche le eccezioni rimangono pressoché le stesse rispetto a quelle della Direttiva; infatti, il Regolamento, esclude dal proprio campo di applicazione i trattamenti di dati personali effettuati:

- per attività che non rientrano nell'ambito di applicazione del diritto UE;

[64] In alcuni casi si applica esclusivamente agli archivi pubblici, come in Brasile; in altri si applica principalmente agli archivi pubblici, ma anche agli archivi privati, come in Argentina.
[65] G. Resta e V. Zeno-Zencovich, *La protezione transnazionale dei dati personali: dai "Safe Harbour Principles" al "Privacy Shield",* Roma Tre Press, 2016.

- dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del Titolo V, capo 2 del TUE[66];
- da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;
- dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

Cambia significativamente, invece, l'ambito di applicazione territoriale. La Direttiva 95/46/CE trova infatti applicazione, tramite le disposizioni nazionali di attuazione, soltanto quando il trattamento è effettuato nel contesto delle attività di uno stabilimento del titolare situato in Unione Europea.

Nel Regolamento 2016/679, invece, la disposizione di riferimento, l'articolo 3, recita così:

1. *Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento dell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.*
2. *Il presente regolamento si applica 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:*

- *l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure*

[66] "Disposizioni specifiche sulla politica estera e di sicurezza comune".

- *il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.*

Tale articolo è innovativo per due diverse ragioni. Innanzitutto, cambia il significato del tradizionale principio di stabilimento: la disciplina trova applicazione indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione; in secondo luogo, l'ambito di applicazione è esteso anche a titolari e responsabili non stabiliti nell'Unione, laddove siano trattati dati personali di interessati che, invece, si trovano nell'UE; questo, però, solo nei casi dei due punti del paragrafo 2.

La ragione di queste novità va individuata nel fatto che le istituzioni europee recepiscono le indicazioni provenienti dalla giurisprudenza della Corte di Giustizia, la quale in alcune sentenze, soprattutto a partire dalla famosissima pronuncia *Google Spain*[67], cerca di estendere l'applicazione della disciplina UE anche a casi in cui i titolari non sono stabiliti nell'Unione e i dati sono trattati principalmente fuori dal territorio della stessa.

Al proposito, si rende necessario, ai fini della nostra analisi, fare un rapido accenno alla sentenza *Google Spain*, in merito al punto in cui tratta della territorialità o meno di un trattamento. Nel 2009 il cittadino spagnolo Mario Costeja Gonzàlez si rese conto che, inserendo il proprio nome nel motore di ricerca del gruppo Google (*Google Search*), l'elenco dei link rimandava a due pagine del quotidiano, anch'esso spagnolo, "*La Vanguardia*", rispettivamente del 19 gennaio e del 9 marzo 1998. Su di esse figurava l'annuncio di una vendita all'asta di immobili in seguito ad un pignoramento effettuato per la riscossione coattiva di

[67] *Google Spain SL, Google Inc vs Agencia Española de Protección de Datos, Mario Costeja Gonzláez*, Corte di Giustizia dell'Unione europea, 13 maggio 2014 (causa C-131/12). All'origine della vicenda vi è una richiesta con la quale un cittadino spagnolo aveva cercato di ottenere, prima dal gestore del sito e poi da Google, la rimozione di alcuni dati personali pubblicati su un articolo di giornale ritenuti non più attuali. L'AEPD (autorità spagnola per la protezione dei dati personali) aveva ordinato a Google di rimuovere i dati in questione, ma Google aveva rifiutato di ottemperare alla richiesta.

crediti previdenziali nei confronti dello stesso signor Gonzàlez. Così, il 5 marzo 2010, l'interessato presentò dinnanzi all'AEPD[68] un reclamo contro "*La Vanguardia Ediciones SL*", nonché contro *Google Spain* e *Google Inc*, affermando che il pignoramento effettuato nei suoi confronti fosse stato interamente definito da svariati anni e che la menzione dello stesso fosse ormai priva di qualsiasi rilevanza. Per questo, da un lato chiese che fosse ordinato a La *Vanguardia* di sopprimere o modificare le pagine suddette affinché i suoi dati personali non vi comparissero più, oppure di ricorrere a taluni strumenti forniti dai motori di ricerca per proteggere tali dati; dall'altro chiese che fosse ordinato a *Google Spain* o a *Google Inc*. di eliminare o di occultare i suoi dati personali, in modo che fossero cessati di comparire tra i risultati di ricerca e non figurassero più nei link di *La Vanguardia*. L'AEPD, nel luglio del 2010, respinse il suddetto reclamo nella parte in cui era diretto contro *La Vanguardia*, ritenendo che la pubblicazione da parte di quest'ultima delle informazioni in questione fosse legalmente giustificata, poiché aveva avuto luogo su ordine del Ministero del Lavoro e degli Affari sociali con lo scopo di conferire il massimo di pubblicità alla vendita pubblica, al fine di raccogliere il maggior numero di partecipanti all'asta. Al contrario, il reclamo venne accolto nella parte in cui era diretto contro *Google Spain* e *Google Inc*. L'AEPD considerò infatti che i gestori di motori di ricerca fossero assoggettati alla normativa in materia di protezione dei dati, poiché essi ne effettuavano un trattamento. Tale autorità ritenne inoltre di essere autorizzata ad ordinare la rimozione nonché il divieto di accesso a taluni dati da parte dei gestori di motori di ricerca, qualora essa ritenesse che la localizzazione e la diffusione degli stessi avrebbero potuto ledere il diritto alla protezione dei dati e la dignità delle persone. L'AEPD affermò infine che tale obbligo poteva incombere direttamente sui gestori dei motori di ricerca, senza che fosse necessario cancellare i dati o le informazioni dal sito web in cui questi compaiono, quando il mantenimento di tali informazioni nel sito in questione fosse giustificato da una norma di legge. Contro la decisione

[68] Agenzia spagnola di protezione dei dati.

dell'AEPD, *Google Spain* e *Google Inc*. proposero due ricorsi separati di fronte *all'Audiencia Nacional*[69]. Tale giudice chiarì che i ricorsi sopra menzionati portavano a chiedersi quali obblighi incombessero sui gestori di motori di ricerca per la tutela dei dati delle persone interessate; la risposta al quesito dipendeva dal modo in cui la Direttiva 95/46/CE fosse interpretata nel contesto delle tecnologie che si svilupparono dopo la sua pubblicazione. Per questo, l'*Audiencia Nacional* sollevò dinanzi alla Corte di Giustizia dell'Unione europea varie questioni pregiudiziali.

Tra le varie questioni pregiudiziali quella riguardante l'ambito di applicazione territoriale è proprio la prima. L'articolo 4 paragrafo 1 lettera a) della Direttiva 95/46/CE richiede che il trattamento sia effettuato nel contesto delle attività di uno "stabilimento" nel territorio dello Stato membro. Nel caso di specie, *Google Spain* è una filiale di *Google Inc*. sul territorio spagnolo: *l'Audiencia Nacional* chiese dunque se esistesse o meno uno "stabilimento" in Spagna. La Corte rispose affermativamente: "qualora il gestore di un motore di ricerca apra in uno Stato membro una succursale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti da tale motore di ricerca e l'attività della quale si dirige agli abitanti di detto Stato membro", si può parlare di "stabilimento" nel Paese in questione.

Il punto di vista della Corte su tale questione pregiudiziale fu analogo a quello precedentemente espresso dall'Avvocato generale Niilo Jääskinen nelle Conclusioni presentate il 25 giugno 2013. Secondo l'Avvocato, infatti, si può parlare di stabilimento a norma dell'articolo 4 paragrafo 1 lettera a) della Direttiva "quando l'impresa che fornisce il motore di ricerca apra in uno Stato membro, ai fini della promozione e della vendita di spazi pubblicitari sul motore di ricerca, un ufficio o una controllata che orienti le proprie attività verso gli abitanti del suddetto Stato", quindi anche nel caso di specie.

[69] È un tribunale speciale che ha la giurisdizione sull'intero territorio spagnolo.

Tornando all'articolo 3 del Regolamento 679/2016, un simile cambiamento, grazie anche agli spunti della sentenza *Google Spain*, pone fine alla pretesa dei *service provider*[70] di sottrarsi alle normative europee e alla giurisdizione degli Stati membri, non viene accolto con particolare favore in quei Paesi extra europei, USA in primis, in cui le garanzie in materia di protezione dei dati personali sono inferiori rispetto a quelle dell'Unione Europea. Le imprese di questi Stati, infatti, se vogliono continuare a trattare dati di interessati che si trovano in Europa, dovranno modificare i propri comportamenti.

La disposizione in esame è completata dall'articolo 27, il quale al paragrafo 1 stabilisce che: "*Ove si applichi l'articolo 3, paragrafo 2, il titolare del trattamento o il responsabile del trattamento designa per iscritto un rappresentante nell'Unione*"[71]. Per analizzare tale disposizione bisogna partire da quanto disposto dal considerando 80 del Regolamento, secondo il quale nel caso in cui un titolare del trattamento non sia stabilito nell'Unione, ma tratti dati personali di interessati che si trovano nell'Unione e le attività di trattamento sono connesse all'offerta di beni o alla prestazione di servizi a tali interessati in Europa, indipendentemente dall'obbligatorietà di un pagamento degli interessati o al controllo del loro comportamento, nella misura in cui tale comportamento ha luogo all'interno dell'Unione, deve individuare un rappresentante in Europa, a norma dell'articolo 27 sopra menzionato. Secondo il principio dell'extraterritorialità, infatti, le disposizioni del Regolamento si applicano indipendentemente dal luogo in cui è situata l'organizzazione, se questa tratta dati personali di cittadini dell'Unione. È anche importante ricordare che il GDPR si rivolge sia ai titolari del trattamento che ai responsabili del trattamento di dati personali[72]. Una società senza stabile organizzazione sul territorio europeo che intende offrire prodotti, beni o servizi a soggetti direttamente o indirettamente identificabili residenti sul

[70] Fornitori di servizi Internet.
[71] L'articolo 27 paragrafo 2 stabilisce invece quali sono i casi in cui l'obbligo del paragrafo 1 non si applica.
[72] Come ad esempio ai fornitori di servizi *cloud*, reti VPN, fornitori di beni immateriali, quali musica, video, immagini vettoriali, software.

territorio europeo è tenuta a soddisfare quanto richiesto dal GDPR. Lo stesso vale per le società non appartenenti all'Unione europea che monitorano il comportamento di cittadini europei, nella misura in cui il loro comportamento si svolge sul territorio dell'UE. A tal fine, dunque, perché una società straniera possa operare sul territorio dell'Unione nel rispetto del Regolamento 679/2016 deve provvedere alla designazione di un rappresentante, ma non sempre tale nomina è obbligatoria. La designazione del rappresentante è infatti esclusa quando:

- i dati personali vengono elaborati solo occasionalmente;
- il trattamento non include il trattamento su larga scala di categorie speciali di dati o dati giudiziari o dati relativi a condanne penali;
- è improbabile che il trattamento comporti un rischio per i diritti e le libertà degli interessati.

Per comprendere quando, ricorrendo i presupposti innanzi delineati specificatamente riferiti alle caratteristiche del trattamento, sia obbligatoria la designazione di un rappresentante, è necessario chiarire il concetto di stabilimento sul territorio dell'Unione, in quanto solo in assenza di stabilimento in uno degli Stati dell'Unione Europea, il titolare/responsabile straniero dovrà provvedere a determinare un ufficio di rappresentanza. Sul punto viene in aiuto il considerando 22 del Regolamento, secondo cui "*lo stabilimento implica l'effettivo e concreto svolgimento di attività nell'ambito di un'organizzazione stabile, ovvero il luogo in cui sono condotte le principali attività di trattamento dei dati sul territorio dell'Unione*"; la forma, non è rilevante. Se dunque una società straniera ha una sede di affari in uno degli Stati dell'Unione Europea, non è necessario che essa nomini un rappresentante in UE, in quanto quella stabile organizzazione fungerà da anello di congiunzione tra l'Autorità di controllo e gli interessati sul territorio; se però la società straniera si rivolge a cittadini dell'Unione solo virtualmente, ma nulla di fisico è presente sul territorio europeo, la casa madre straniera dovrà provvedere ad individuare un ufficio di rappresentanza in loco, sempre che non si

trovi nelle situazioni di cui all'articolo 27 per cui è prevista l'esclusione dalla individuazione del rappresentante.

Il rappresentante deve essere espressamente designato mediante mandato scritto del titolare del trattamento o del responsabile del trattamento che deve prevedere espressamente la possibilità per questi di agire per conto di questi ultimi con riguardo agli obblighi che ad essi derivano dal Regolamento. La designazione di tale rappresentante non incide sulla responsabilità generale che resta in capo al titolare del trattamento o del responsabile del trattamento ai sensi del Regolamento. Il rappresentante è tenuto a svolgere i suoi compiti nel rispetto del mandato conferitogli, anche per quanto riguarda la cooperazione con le autorità di controllo competenti per qualsiasi misura adottata al fine di garantire il rispetto del regolamento; egli infatti è incaricato dal titolare del trattamento o dal responsabile del trattamento a fungere da interlocutore, in sua aggiunta o in sua sostituzione, in particolare delle autorità di controllo e degli interessati, per tutte le questioni riguardanti il trattamento. Inoltre, il rappresentante dovrebbe essere oggetto di misure attuative in caso di inadempienza da parte del titolare del trattamento o del responsabile del trattamento che lo ha designato, a tal proposito, è opportuno prevedere sanzioni disciplinari nel contratto di mandato.

Il rappresentante dovrà rispondere per conto del titolare/responsabile del trattamento alle richieste degli interessati, pertanto, sarebbe opportuno scegliere un soggetto che sia in grado di interloquire in diverse lingue, inoltre dovrà collaborare con le diverse autorità di vigilanza e si dovrà occupare della conservazione dei documenti relativi alle attività di trattamento svolte, anche qualora siano richiesti in sede di ispezione.

2.2.1 Definizioni: tradizione e innovazione

Un'altra norma fondamentale del Capo I, dedicato alle disposizioni generali, è l'articolo 4, rubricato "definizioni". Tale disposizione corrisponde al

vecchio articolo 2 della Direttiva 95/46/CE, ma l'elenco ivi contenuto è molto più ampio e completo comprendendo un totale di 26 termini. In particolar modo risultano nuove le definizioni di: pseudonimizzazione, profilazione, limitazione di trattamento, violazione dei dati personali, 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, dati genetici, dati biometrici, dati relativi alla salute. Molte definizioni sono state, invece, soltanto modificate, si tratta di: dato personale, trattamento, titolare del trattamento, responsabile del trattamento, destinatario. In continuità con la normativa ancora vigente risultano essere le nozioni di: archivio, terzo, consenso dell'interessato.

Il Regolamento definisce il "dato personale" come "*qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*". Tale definizione non è nuova, e difatti ricalca quella data in passato dalla Direttiva 95/46/CE nel suo articolo 2. Dalla lettura delle norme, "dato personale" e "informazione" sembrerebbero coincidere, ma in realtà sono concetti differenti: si può affermare che il dato è la fonte dell'informazione, nel quale questa è contenuta e dal singolo dato o dall'insieme di dati da cui l'informazione può essere estratta o inferita. L'informazione non coincide col dato, poiché ne è l'elaborazione.

L'avvento della società digitale ha provocato un ampliamento notevole delle tipologie di dati che possono essere oggetto di trattamento, e un simile ampliamento ha, allo stesso tempo, reso più vasta anche la tutela riconosciuta al singolo e al suo patrimonio di informazioni; la stessa espressione "qualunque informazione", conferisce alla nozione di dato la massima portata. Rimangono

fuori dal campo di applicazione della normativa sulla protezione dei dati personali il trattamento di dati "non personali", come ad esempio i dati anonimi o il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali.

Importanti nella definizione di dato personale sono le espressioni "qualsiasi informazione", "concernente", "identificata o identificabile", "persona fisica". L'espressione "qualsiasi informazione" fa emergere chiaramente la volontà del legislatore di fornire un ampio concetto di dati personali, e può trattarsi di informazioni tanto di natura soggettiva quanto di natura oggettiva. L'aggettivo "qualsiasi" fa comprendere ulteriormente l'ampiezza della nozione. Il secondo elemento è la locuzione "concernente", essenziale soprattutto in relazione ai nuovi sviluppi tecnologici, che hanno ampliato la portata delle informazioni che possono riguardare una determinata persona. Vengono definiti tre fattori alternativi: il contenuto, ossia il fatto che un dato riguardi direttamente una persona; la finalità, ossia il fatto che il dato venga usato per valutare una persona o per condizionare i suoi comportamenti; il risultato, ossia che l'utilizzo del dato comporti un impatto sui diritti di quella persona. Il terzo elemento da sottolineare è "identificata o identificabile", il quale rappresenta una condizione della persona, rispettivamente effettiva o possibile. Non è sufficiente l'astratto collegamento con una persona, ma occorre che quest'ultima sia singolarmente individuata o individuabile. Diversamente, si avrà un'informazione anonima. Sul concetto di "persona fisica" ci si riferisce a persone fisiche viventi, ma è da evidenziare il fatto che i dati dei defunti e dei nascituri possono in taluni casi beneficiare di protezione[73]. Per esempio in Italia, in seguito all'entrata in vigore del D.Lgs. 101/2018, i diritti aventi ad oggetto i dati delle persone decedute possono essere esercitati da chi ne ha interesse.

Tra le nuove definizioni dettate dal Regolamento UE 2016/679, sempre all'interno dell'articolo 4, possiamo trovare quelle di "dati genetici", "dati

[73] Nell'ordinamento italiano viene data protezione in taluni casi a dati concernenti nascituri e morti.

biometrici" e "dati relativi alla salute". I "dati genetici" sono "*dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sullo stato di salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione*". I "dati biometrici" sono invece "*dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici*". Infine i "dati relativi alla salute" sono "*i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relativa al suo stato di salute*". A differenza della nozione di dato personale, la quale come abbiamo potuto evidenziare risulta molto ampia, queste nuove categorie di dati sembrano invece molto simili tra loro, essendo tutte e tre rivolte alla salute fisica della persona e differenziandosi tra loro minimamente.

In origine esistevano tre categorie di dati: dati personali, dati giudiziari e dati sensibili. Tra i dati sensibili rientravano le categorie particolari quali quelle di dati biometrici, dati genetici e danni relativi alla salute. Con il Regolamento 679/2016 esiste un'unica categoria di dati, quella di "dati personali", dalla quale possiamo estrapolare i dati genetici, biometrici e relativi alla salute. Non vi è più alcun riferimento esplicito ai dati sensibili e ai dati giudiziari.

L'articolo 4 del GDPR parla anche di "trattamento" dei dati e si allinea nuovamente alla disciplina della Direttiva 95/46/CE, definendolo come: "*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*". Dalla lettura della definizione si evince che la nozione di

trattamento riguarda sia una singola operazione che un complesso di operazioni che hanno ad oggetto i dati personali; è sufficiente quindi, affinché di trattamento possa parlarsi, che anche una sola delle operazioni elencate venga posta in essere, anche in assenza di una banca dati[74]. Il Regolamento si applica sia al trattamento dei dati con mezzi informatici sia al trattamento effettuato con altri mezzi, come ad esempio quelli cartacei, e rivela la sua piena natura di normativa sull'uso delle informazioni piuttosto che sulla tutela della riservatezza in senso stretto. Ciò che costituisce oggetto della tutela non è l'informazione riservata, bensì il dato, qualunque natura esso abbia, se riferibile a persona fisica, e la medesima ampiezza definitoria ha il trattamento: qualunque operazione effettuata sui dati.

Immediatamente successiva alla definizione di trattamento, possiamo trovare quella nuova di "limitazione di trattamento", ovvero "*il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro*".

Dopo aver parlato di trattamento, se l'attenzione si sposta al punto 23) dell'articolo 4 del Regolamento, si può rinvenire la definizione di "trattamento transfrontaliero", la quale prevede due casi: nel primo caso si tratta di un trasferimento di dati tra più Stati membri dell'Unione europea, nella seconda ipotesi di un trattamento di dati che incide o che potrebbe incidere in modo sostanziale su interessi situati in più di uno Stato membro dell'Unione. Se si è in presenza di un trattamento di dati transfrontaliero è fondamentale individuare l'autorità di controllo capofila, competente a sorvegliare sulla conformità di tale trattamento cosicché possa gestire eventuali reclami da parte degli interessati relativi al trasferimento. L'autorità di controllo capofila è quella dello stabilimento principale del titolare del trattamento o del responsabile o quella dello Stato UE in cui è situato l'unico stabilimento del titolare o del responsabile del trattamento.

Passando alla trattazione dei soggetti nell'ambito del trattamento, possiamo subito accorgerci del fatto che nell'ampio elenco delle definizioni fornite dal Regolamento è assente quella di "interessato", soggetto passivo del

[74] Questa è la grande differenza rispetto al testo dell'articolo 2 lettera b) della Direttiva 95/46/CE.

trattamento, che però è ricavabile attraverso quella di dato personale. Innanzitutto, sicuramente l'interessato è una persona fisica, dopodiché deve essere identificato o identificabile attraverso una serie di identificatori, come ad esempio il nome, l'ubicazione, o dati di natura virtuale o genetica. Sugli identificativi si sofferma il considerando numero 30[75]. La qualità di interessato cessa con la morte della stessa, ma è previsto che gli Stati membri possano prevedere norme riguardanti il trattamento dei dati dei deceduti, stessa cosa che riguarda i nascituri. L'interessato è il centro di imputazione di una serie di interessi ed è il soggetto che può, attraverso il consenso, porre in essere uno dei presupposti di legittimità di trattamento.

La nozione di "consenso dell'interessato" presente nel Regolamento risulta arricchita rispetto a quella presente nella Direttiva 95/46/CE: il consenso è "*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*". L'atto di manifestazione della volontà è dunque necessario, e l'assenso dell'interessato a che i dati personali che lo riguardano siano oggetto di trattamento può prevedere qualsiasi tipo di manifestazione. In assenza di un comportamento attivo dell'interessato, è difficile per il titolare del trattamento stabilire se il silenzio dello stesso significhi accettazione o consenso. Il consenso, naturalmente, può essere valido soltanto se l'interessato sia in grado di operare realmente una scelta, e non ci sia il rischio di raggiri, intimidazioni, coercizioni o conseguenze negative significative nel caso in cui questa persona non manifesti il proprio consenso: questo è quanto si intende con la dicitura "consenso libero". Il consenso può essere effettivamente libero solo

[75] "Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, a marcatori temporanei (*cookies*) o a identificativi di altro tipo, come i *tag* di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle".

se si presenta come manifestazione del diritto all'autodeterminazione informativa e dunque al riparo da qualsiasi pressione. Per essere valido, il consenso deve anche essere "specifico", ovvero comprensibile: dovrebbe cioè riferirsi chiaramente e precisamente al campo di applicazione e alle conseguenze del trattamento dei dati. Non può riferirsi ad un insieme illimitato di attività di trattamento, poiché il contesto al quale si applica è limitato. Inoltre il consenso deve essere "informato", cioè basato sulla valutazione e comprensione dei fatti e sulle conseguenze di una determinata azione, e l'interessato dunque deve ricevere, in modo comprensibile e chiaro, informazioni precise e complete su tutti gli aspetti rilevanti. Per garantire un'informazione adeguata dunque bisogna fare riferimento a due tipi di obblighi: qualità dell'informazione e accessibilità e visibilità delle informazioni. Infine il consenso deve essere "inequivocabile", nel senso che la manifestazione con la quale l'interessato manifesta il proprio assenso al trattamento dei suoi dati personali non deve lasciare spazio ad ambiguità per quanto concerne la sua intenzione.

Passando alla trattazione dei soggetti attivi del trattamento, al vertice di quella che è l'attività di trattamento dei dati è posto il titolare del trattamento, la cui definizione si ritrova al numero 7 dell'articolo 4 del Regolamento, che lo definisce come "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri*". Il primo elemento della definizione si riferisce al soggetto chiamato a rispondere degli obblighi derivanti dal Regolamento, ovvero persone fisiche, giuridiche o qualsiasi altro organismo. Un secondo elemento è rappresentato dalla locuzione "singolarmente o assieme ad altri", e si tratta di casi in cui il trattamento di dati personali veda interagire più figure. Tuttavia, la parte di maggiore rilevanza della definizione di titolare del trattamento è rappresentata dall'espressione "determina

le finalità e i mezzi del trattamento di dati personali". Innanzitutto, l'attribuzione della qualifica di titolare del trattamento è un fatto, e non occorre alcuna formalizzazione della titolarità, pertanto, non è richiesta una specifica attribuzione per legge, discendendo la stessa da elementi fattuali o dalle circostanze. Essere titolare del trattamento deriva, quindi, dal fatto concreto che un'entità ha scelto di trattare dati personali per propri fini.

La successiva parte della definizione, "finalità e mezzi del trattamento", rappresenta la parte sostanziale del testo, ovvero cosa deve determinare una parte per essere qualificata quale titolare del trattamento. È stato affermato che determinare le finalità e gli strumenti equivale a determinare, rispettivamente, il perché e il come di certe attività di trattamento. Per quanto riguarda i mezzi invece, con tale termine non ci si riferisce solo ai mezzi tecnici per trattare i dati personali, ma anche alle modalità attraverso le quali il trattamento è effettuato. Quindi mentre la determinazione delle finalità del trattamento farebbe scattare in ogni caso la qualifica di titolare del trattamento, la determinazione degli strumenti implicherebbe una titolarità solo qualora riguardi gli aspetti fondamentali dei mezzi stessi.

In ruolo subalterno rispetto al titolare del trattamento si pone il responsabile del trattamento, definito dal Regolamento come "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*". Si tratta di un concetto sostanzialmente immutato rispetto alla Direttiva del 1995. Analogamente a quanto avviene per la definizione di titolare del trattamento, anche questa definizione prevede una vasta gamma di soggetti. Per poter agire come responsabile del trattamento occorrono due requisiti: essere una persona fisica o giuridica distinta dal titolare del trattamento ed elaborare i dati personali per conto di quest'ultimo. L'elemento più importante della definizione è la condizione secondo cui il responsabile del trattamento interviene per conto del titolare del trattamento, poiché richiama il concetto di delega. Pertanto, la liceità dell'attività di trattamento dei dati da parte del responsabile del trattamento è determinata dal mandato

ricevuto dal titolare del trattamento: se va al di là del proprio mandato e se acquisisce un ruolo rilevante nella determinazione delle finalità o degli aspetti fondamentale degli strumenti del trattamento, il responsabile diventa contitolare.

A completare l'ambito dei soggetti si colloca la figura del "destinatario", definito come "*la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento*". Anche questa definizione non si discosta da quella contenuta nella Direttiva n. 46; elemento caratterizzante di tale figura è quello della ricezione della comunicazione di dati personali.

Il Regolamento, come in precedenza la Direttiva, si preoccupa anche di fornire una definizione di "Terzi", stabilendo che tali non includono l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento. Emerge dalla definizione fornita che terzo è la persona che non ha alcun rapporto con nessuno dei soggetti che a vario titolo sono coinvolti nel trattamento dei dati. Inoltre il Terzo si differenzia dal destinatario perché non riceve alcuna comunicazione di dati in ragione della posizione giuridica che esso ha rispetto alle figure che effettuano i trattamenti o che sono da esse interessate.

Un cenno va fatto anche alla figura del "rappresentante", che è "*la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento*".

Importanti figure tra i soggetti sono quei soggetti aventi funzioni di controllo, tra i quali si colloca, *in primis*, l'autorità di controllo, che è "*l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51*".

Tale figura è distinta da quella di autorità di controllo interessata, per la quale si intende "*un'autorità di controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure, c) un reclamo è stato proposto a tale autorità di controllo*".

Dopo aver trattato le definizioni ritenute fondamentali tra le 26 previste dal presente articolo 4, si può proseguire con l'analisi del Regolamento.

2.3 Capo II: principi

Il Capo II del Regolamento 2016/679, che va dall'articolo 5 all'articolo 11, è dedicato ai "Principi". La norma di apertura di tale Capo ricalca molto l'articolo 6 della Direttiva 95/46/CE. L'articolo 5 del Regolamento, rubricato "Principi applicabili al trattamento di dati personali" contiene infatti un elenco di tutti i principi governanti la materia, e, per la sua importanza, merita di essere riportato:

1. *I dati personali sono:*

- *trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza")*[76]*;*
- *raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente*

[76] "Lawfulness, fairness and transparency".

all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali ("limitazione della finalità")[77]*;*

- *adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati")*[78]*;*
- *esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza")*[79]*;*
- *conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato ("limitazione della conservazione")*[80]*;*
- *trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ("integrità e riservatezza")*[81].

2. *Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo ("responsabilizzazione")*[82].

Le differenze più significative tra l'articolo sopra riportato e l'articolo 6 della Direttiva 95/46/CE sono due: l'introduzione della lettera f), dedicata ai

[77] "Purpose limitation".
[78] "Data minimisation".
[79] "Accuracy".
[80] "Storage limitation".
[81] "Integrity and confidentially".
[82] "Accountability".

principi di integrità e riservatezza, ma soprattutto l'aggiunta, alla lettera a), del principio di trasparenza. Nella sua opera di riforma, il legislatore europeo si dimostra particolarmente attento a quest'ultimo principio, poiché non solo lo introduce all'articolo 5, ma dedica ad esso un'apposita sezione. Tale sezione, la numero 1 del Capo III ("Trasparenza e modalità"), è costituita da un unico articolo, l'articolo 12, il quale accresce gli obblighi di trasparenza in capo al titolare del trattamento.

Rimanendo al Capo II, l'articolo 6, rubricato "liceità del trattamento", invece specifica uno dei principi enunciati nell'articolo 5 paragrafo 1 lettera a): il principio di liceità; tale paragrafo è quasi una trasposizione letterale rispetto alla Direttiva n. 46. Va ricordato che, affinché il trattamento sia lecito, deve essere presente almeno una delle condizioni elencate nell'articolo in questione: la lettera a) fa riferimento all'ipotesi in cui "*l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità*"; le lettere dalla b) alla f), invece, elencano casi in cui il trattamento è comunque lecito nonostante la mancanza del consenso dell'interessato, in virtù di un altro fondamento giuridico. Nello specifico: b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) il trattamento è 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; f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Una novità significativa, invece, è costituita dall'articolo 7 del Regolamento, "condizioni per il consenso", che precisa, ai fini della liceità del

trattamento, quali sono le condizioni alle quali l'interessato può manifestare e revocare il proprio consenso. Innanzitutto, "*qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali*". Dopodiché, se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Con la stessa facilità con cui è stato accordato il consenso, poi, deve essere possibile revocarlo; il diritto di revoca può essere di conseguenza esercitato in qualsiasi momento, ma la revoca del consenso non pregiudica la liceità del trattamento basato sul consenso anteriore rispetto alla revoca stessa, e di questo è informato l'interessato ancor prima di esprimere il consenso. Come già evidenziato precedentemente, estremamente significativo è il paragrafo 1, il quale pone in capo al titolare del trattamento l'onere della prova che l'interessato abbia prestato il proprio consenso al trattamento dei suoi dati personali.

Altra disposizione importante, nonché parzialmente innovativa, è l'articolo 9, rubricato "trattamento di categorie particolari di dati personali", che detta un regime specifico per alcuni dati sensibili: il contesto in cui sono trattati, infatti, potrebbe comportare rischi significativi per i diritti e le libertà degli interessati. L'articolo 9 del Regolamento ha come suo "predecessore" l'articolo 8 della Direttiva 95/46/CE, il quale al paragrafo 1 fa riferimento ad un divieto di trattare "*dati personali che rivelino l'origine razziale o etnica, le opinioni pubbliche, 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*". Da evidenziare che il paragrafo 2 dell'articolo 9 del Regolamento elenca situazioni in cui invece il trattamento dei sopracitati dati sensibili è autorizzato.

Va sottolineato come il Regolamento lasci agli Stati membri un margine di discrezionalità piuttosto ampio relativamente al mantenimento o introduzione di ulteriori condizioni o limitazioni con riguardo al trattamento di particolari dati sensibili, come i nuovi dati genetici, biometrici e quelli relativi alla salute.

Nella stessa prospettiva della disposizione appena presa in considerazione si pone l'articolo precedente, il numero 8, rubricato "condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione", che rappresenta invece un elemento di novità più significativo, non essendovi una corrispondente disposizione nella Direttiva 95/46/CE. Tale norma detta infatti, per quanto riguarda l'offerta diretta ai servizi della società dell'informazione ai minori, un regime di particolare tutela: il trattamento di dati è lecito ove il minore che esprime il proprio consenso abbia almeno 16 anni. Altrimenti, il consenso deve essere prestato o autorizzato dal titolare della responsabilità genitoriale. In Italia, in seguito all'entrata in vigore del D.Lgs. 101/2018, la soglia d'età è stata abbassata a 14 anni.

L'ultimo articolo di questo Capo II da menzionare è il numero 10, rubricato "trattamento dei dati personali relativi a condanne penali e reati", che si inserisce nel medesimo solco dei due precedenti, e che ha come suo "predecessore" l'articolo 8 paragrafo 5 della Direttiva del 1995. Qui si prevede che, per quanto riguarda i dati relativi a condanne penali e a reati o a misure di sicurezza connesse, il trattamento deve avvenire sotto il controllo dell'autorità pubblica oppure in presenza di "adeguate garanzie": dunque per quanto riguarda questi dati, a differenza di ciò che avviene per tutti gli altri dati sensibili, la tutela accordata dagli strumenti di diritto UE è simile a quella della Convenzione 108 del 1981.

2.4 Capo III: diritti dell'interessato

Il Capo III del Regolamento 2016/679 UE riguarda i "Diritti dell'interessato", dei quali alcuni sono meglio definiti rispetto al passato, altri sono

invece introdotti *ex novo*. L'interessato non è un soggetto che passivamente subisce le operazioni di trattamento effettuate sui propri dati personali, anzi, questi vanta un ampio potere di controllo e di intervento sui dati personali che si declina lungo specifiche prerogative, esercitabili senza particolari formalità. Attraverso il controllo sulle proprie informazioni, la persona determina le modalità di costruzione della propria dimensione individuale. Sotto questo profilo, i diritti dell'interessato rappresentano declinazioni della più generale pretesa del singolo di "potersi proiettare liberamente nel mondo attraverso le proprie informazioni, mantenendo però il controllo sul modo in cui queste circolano e vengono utilizzate, indipendentemente dalla sussistenza di una violazione"[83].

La prima disposizione del presente capo è l'articolo 12, che conferma e specifica notevolmente il "diritto all'informazione", legato a doppio filo agli obblighi di trasparenza posti in capo al titolare del trattamento. Tra gli aspetti più significativi:

- si richiede al titolare del trattamento di rendere all'interessato informazioni sulle operazioni di trattamento "*in forma concisa, trasparente, intellegibile, e facilmente accessibile, con un linguaggio semplice e chiaro*". Ciò soprattutto al fine di permettere la consapevolezza di ciò che potrà accadere ai dati e agevolare l'esercizio dei diritti da parte dell'interessato;
- si richiede che le informazioni siano fornite per iscritto o con modalità elettroniche; l'informativa in forma orale è ammessa a due condizioni: deve esserci una richiesta dell'interessato e l'identità dell'interessato deve essere comprovata con altri mezzi;
- si prevede che il titolare, qualora non dia seguito alla richiesta dell'interessato, lo informi senza ritardo (al massimo entro un mese) dei motivi dell'inottemperanza, nonché della possibilità di fare reclamo davanti all'autorità nazionale di controllo e di proporre ricorso giurisdizionale;

[83] *Intervista su privacy e libertà*, Rodotà S., a cura di Paolo Conti, 2005.

- si prevede che, se le richieste dell'interessato sono manifestamente infondate o eccessive il titolare può o addebitare un contributo spese ragionevole o rifiutarsi di soddisfare la richiesta, ma, in tal caso, l'onere della prova ricade sul titolare.

Gli articoli 13 e 14, invece, individuano rispettivamente quali sono le "informazioni da fornire qualora i dati personali siano raccolti presso l'interessato" e le "informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato"[84], e corrispondono agli articoli 10 e 11 della Direttiva 95/46/CE.

Subito dopo troviamo l'articolo 15, il quale parla del "*diritto di accesso dell'interessato", e prevede che "l'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali*"[85], nonché ad ulteriori informazioni elencate dal paragrafo 1. Il diritto in questione, che a sua volta è un elemento imprescindibile del diritto alla protezione dei dati personali, è disciplinato anche dall'articolo 12 lettera a) della Direttiva 95/46/CE e dall'articolo 13 delle Linee guida OCSE.

Strettamente correlato all'articolo 15 è l'articolo 16 del Regolamento, che rappresenta anche una novità rispetto al passato, poiché prevede per l'interessato il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. L'interessato ha, inoltre, il diritto di ottenere l'integrazione dei dati personali incompleti.

[84] Tra le informazioni che figurano sia all'articolo 13 che all'articolo 14 possiamo trovare, ad esempio: l'identità e i dati di contratto del titolare del trattamento, le finalità nonché la base giuridica del trattamento, gli eventuali destinatari dei dati personali.
[85] Tra le informazioni dell'articolo 15 paragrafo 1 possiamo evidenziare, a titolo esemplificativo: le finalità del trattamento, le categorie di dati personali in questione, i destinatari a cui i dati personali sono stati o saranno comunicati, il periodo di conservazione dei dati personali previsto.

2.4.1 Diritto all'oblio

Uno degli elementi di maggior interesse dell'intero Regolamento è rappresentato dall'articolo 17, il quale disciplina il "diritto alla cancellazione" dei dati personali, detto anche "diritto all'oblio". A tal proposito, data l'importanza di tale disposizione, ne va citato il testo:

1. *L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:*

- *i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;*
- *l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;*
- *l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;*
- *i dati personali sono stati trattati illecitamente;*
- *i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;*
- *i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.*

2. *Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati*

personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

3. *I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:*

- *per l'esercizio del diritto alla libertà di espressione e di informazione;*
- *per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;*
- *per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), dell'articolo 9, paragrafo 3;*
- *a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi o di tale trattamento; o*
- *per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.*

Questa norma, così come l'articolo 16, ha come suo predecessore l'articolo 12 della Direttiva 95/46/CE, ma ovviamente detta una disciplina molto più articolata rispetto ai precedenti strumenti giuridici. In base al primo paragrafo, la cancellazione può essere chiesta e ottenuta da parte dell'interessato in tutta una serie di situazione tassativamente elencate, poiché, in questi casi, il titolare ha l'obbligo di cancellare i dati senza indebito ritardo.

L'articolo in questione recepisce, parzialmente, la giurisprudenza della Corte di Giustizia dell'Unione europea esplicitata nella nota sentenza *Google Spain* del 13 maggio 2014. Nell'articolo sopracitato, paragrafo 1, lettera a), possiamo trovare l'ipotesi a cui fa riferimento la sentenza in questione, quando

afferma che il trattamento inizialmente lecito di dati esatti può diventare, col passare del tempo, incompatibile con la Direttiva del ’95 qualora tali dati non siano più necessari in rapporto alle finalità per le quali sono stati raccolti o trattati e che, in questo caso, deve essere garantito il diritto all’oblio.

L’aspetto più innovativo della disposizione, però, è certamente il paragrafo 2, che trae spunto dall’articolo 12 della Direttiva del 1995, ma va ben oltre, sancendo che, qualora il titolare del trattamento abbia reso conoscibili a tutti i dati personali, diffondendoli a titolo di pubblicazione (cosa che in rete si verifica ogni giorno), egli è obbligato a informare gli altri titolari, che stanno trattando tali dati, “della richiesta dell’interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali”. I dati pubblicati su Internet sono messi a disposizione di un numero illimitato e indefinito di destinatari e di ulteriori titolari; altri utenti potrebbero scaricare i dati in questione sui loro dispositivi e inviarli nuovamente. Quindi, è praticamente impossibile rintracciare tutti questi dati e tutti gli ulteriori titolari. A tal proposito, il paragrafo 2 per l’appunto, prevede che le misure, anche tecniche, per informare gli altri titolari della richiesta di cancellazione siano “ragionevoli”, tenendo conto della tecnologia disponibile e dei relativi costi. Il cuore del diritto all’oblio è proprio questo paragrafo 2 del GDPR, nella sua attuale formulazione, che obbliga il titolare ad adottare misure ragionevoli per informare gli altri titolari della richiesta di cancellazione anche nel caso di trattamento originariamente lecito. Senza tale disposizione, che è in linea anche con la giurisprudenza *Google Spain*, non possiamo certo utilizzare l’espressione “diritto all’oblio”, neanche in senso lato o come sinonimo di “diritto alla cancellazione”.

L’articolo in questione, infine, ha anche un paragrafo 3, il quale prevede che il diritto all’oblio non sussista in tutta una serie di casi, ritenuti eccezionali.

In conclusione, però, l’articolo 17 non rappresenta, nell’ottica degli interessati, un passo avanti, ma piuttosto un passo indietro rispetto alla sentenza *Google Spain*: il diritto sancito in tale disposizione, infatti, è sottoposto a condizioni, soffre numerose eccezioni, soccombendo di fronte alla libertà di

espressione e di informazione, e può essere fatto valere esclusivamente nei confronti dell'editore della pagina web.

In sintonia con quanto affermato sinora, si pone la dottrina della giurista Finocchiaro, secondo la quale "la norma in questione utilizza l'espressione diritto all'oblio, denominazione affascinante, provocatoria, e forse demagogica, ma senza che ve ne sia la reale necessità: siamo di fronte ad un semplice diritto alla cancellazione, meglio precisato e dalla portata più ampia rispetto alla Direttiva 95/46/CE, ma pur sempre tale. In sintesi, siamo di fronte ad un nuovo abito per un vecchio diritto"[86].

2.4.2 Diritto alla limitazione, alla portabilità e di opposizione

Giunti a questo punto va fatta una menzione all'articolo 18 del Regolamento, il quale elenca tassativamente i casi in cui l'interessato ha diritto alla limitazione del trattamento da parte del titolare dello stesso.

Il Regolamento definisce la limitazione del trattamento come "*il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro*". Si tratta, quindi, di misure che consistono nel contrassegnare i dati personali conservati dal titolare che, a fronte di una richiesta dell'interessato, si trovi a dover in qualche modo riconoscere e segregare quei dati che non potrà più trattare in futuro. Il correlato diritto dell'interessato, "diritto di limitazione del trattamento", di cui si parlerà successivamente in maniera più approfondita, è disciplinato dagli articoli 18 e 19 del Regolamento, mentre le misure da prendere sono descritte dal considerando 67.

Le modalità per limitare il trattamento dei dati personali sono individuate nel predetto considerando in maniera esemplificativa e non tassativa e consistono:

[86] G. Finocchiaro, *Il diritto all'oblio nel quadro dei diritti della personalità.*, in: Il diritto all'oblio su internet dopo la sentenza Google Spain, Roma, Roma TrE-Press, 2015.

- nel trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento;
- nel rendere i dati personali selezionati inaccessibili agli utenti;
- nel rimuovere temporaneamente i dati pubblicati da un sito web.

Nel medesimo considerando viene inoltre evidenziato che, negli archivi automatizzati, la limitazione del trattamento dei dati personali dovrebbe, in linea di massima, essere assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati. Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato. Dal punto di vista dell'interessato, si può dire che la limitazione del trattamento si avvicina molto al blocco dei dati, presente nella nostra attuale normativa, dal quale tuttavia si discosta per l'obbligo imposto al titolare di provvedere al contrassegno dei dati il cui trattamento è stato limitato, volto a garantire che la restrizione operata su tali trattamenti sia rispettata anche in futuro.

Il diritto di limitazione del trattamento può essere richiesto dall'interessato nei casi descritti dall'articolo 18 del Regolamento, ovvero quando:

- l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza degli stessi;
- il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
- nonostante il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- l'interessato si è opposto a un trattamento (necessario per l'esecuzione di un compito di interesse pubblico o basato sul legittimo interesse del titolare, compresa la profilazione), in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Quando il titolare proceda a limitare il trattamento, tali dati personali sono trattati solo per la conservazione, e ulteriori trattamenti saranno possibili soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro. Inoltre quando l'interessato ha ottenuto la limitazione del trattamento, nel caso in cui la limitazione venga revocata egli deve essere informato dal titolare del trattamento prima che la revoca abbia effetto. Infine, nel caso in cui i dati personali oggetto di limitazione siano stati comunicati ad altri soggetti, è onere del titolare del trattamento (esattamente come avviene nel caso di diritto all'oblio o alla rettifica) darne comunicazione a ciascuno dei destinatari, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. In ogni caso, il titolare del trattamento è tenuto a comunicare tali destinatari all'interessato che ne faccia richiesta.

Di nuova introduzione, e quindi meritevole di particolare attenzione, è poi il "diritto alla portabilità dei dati", disciplinato dall'articolo 20 del Regolamento. L'interessato ha il diritto di ottenere "in un formato strutturato, di uso comune e leggibile da dispositivo automatico di dati personali che lo riguardano" detenuti dal titolare. Inoltre ha il diritto di trasmetterli da un titolare (come un *social network*, un provider di posta elettronica, una società telefonica, per fare gli esempi di situazioni in cui è più probabile che venga esercitato questo diritto) a un altro titolare, senza impedimenti da parte di colui al quale erano stati forniti precedentemente, in modo da poterli ulteriormente utilizzare. Il diritto in questione si colloca nell'ottica di garantire agli interessati un maggior controllo sui propri dati. A tal proposito è importante il Considerando 68, che recita: "*per rafforzare ulteriormente il controllo sui propri dati è opportuno anche che l'interessato abbia il diritto, qualora i dati personali siano trattati con mezzi automatizzati, di ricevere in un formato strutturato, di uso comune, leggibile da dispositivo automatico e interoperabile i dati personali che lo riguardano che abbia fornito a un titolare*

del trattamento e di trasmetterli a un altro titolare del trattamento. È opportuno incoraggiare i titolari del trattamento a sviluppare formati interoperabili che consentano la portabilità dei dati".

Altra discrepanza rispetto alla precedente disciplina è il riferimento, ora esplicito, alla profilazione. Essa è definita dall'articolo 4, menzionato in precedenza, 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*". Le condizioni di liceità di tale pratica sono enunciate dall'articolo 22, dedicato al "processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione". Tale disposizione trova le proprie radici nell'articolo 15 della Direttiva 95/46/CE, che chiaramente non faceva riferimento alla profilazione, bensì solo alla decisioni individuali automatizzate. L'articolo 22 paragrafo 1 sancisce la regola generale in base alla quale l'interessato ha un vero e proprio "*diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*". Il paragrafo 2 stabilisce, invece, in quali casi la norma di portata generale non si applica, mentre i paragrafi 3 e 4 evidenziano rispettivamente i casi in cui è richiesto anche un intervento umano e le esclusioni di particolari categorie di diritti.

La Sezione 4 del Capo III, oltre a disciplinare il processo decisionale automatizzato relativo alle persone fisiche, contiene anche l'articolo 21, rubricato "diritto di opposizione". L'interessato ha il diritto di opporsi al trattamento:

- "*per motivi connessi alla sua situazione particolare*", che a sua volta si può verificare solo nel caso in cui la condizione che rende il trattamento lecito sia una delle seguenti: a) il trattamento è 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; b) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento di terzi. In questi casi il titolare del trattamento, a seguito dell'opposizione, si astiene dal trattare ulteriormente i dati personali, "*salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria*";

- qualora i dati personali siano trattati per finalità di marketing diretto, il diritto di opposizione è incondizionato.

Il Capo III si conclude con l'articolo 23, in base al quale è possibile limitare, mediante misure legislative, la portata dei diritti fin qui esaminati. Affinché ciò avvenga, è necessario che "*tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare*" interessi e beni come, ad esempio, la sicurezza nazionale, la difesa, la sicurezza pubblica, o anche la prevenzione, l'indagine, l'accertamento e il perseguimento di reati, ed altri tassativamente elencati.

A tal proposito, il Regolamento 679/2016 ha introdotto il concetto di legittimo interesse del titolare quale base giuridica su cui valutare la liceità delle operazioni di trattamento di dati personali. Si tratta di un concetto nuovo e specifico per questo campo, e, di conseguenza, diverso dal legittimo interesse già presente e conosciuto all'interno dell'ordinamento giuridico italiano. Il perseguimento di un legittimo interesse si pone come base giuridica alternativa alle altre previste nell'articolo 6 del GDPR. Il titolare che abbia un legittimo interesse può procedere al trattamento anche in assenza del consenso da parte dell'interessato, di un rapporto contrattuale, di obblighi legali, di esigenze di salvaguardia di interessi vitali dell'interessato o di altra persona fisica, di esercizio di poteri pubblici.

Trattandosi di un nuovo istituto appare utile, per comprenderne la portata e le modalità di attuazione, rifarsi ai considerando contenuti nel medesimo Regolamento che espressamente menzionano le ragioni per cui è stato introdotto e propongono esempi concreti di sua applicazione. In particolare, il considerando 47 chiarisce che per la valutazione della sussistenza di un legittimo interesse del titolare deve innanzitutto tenersi conto delle "*ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento*". Tale valutazione, che nell'impostazione del Regolamento europeo è svolta autonomamente dal titolare, deve quindi basarsi su ciò che l'interessato potrebbe ragionevolmente attendersi rispetto al trattamento dei propri dati da parte del titolare con cui abbia rapporti, o venga in contatto.

Il GDPR elenca anche alcuni esempi di legittimo interesse, tra cui il rapporto cliente/fornitore o tra datore di lavoro e dipendente, situazioni in cui è evidente che l'interessato non può aspettarsi che venga effettuato il trattamento dei propri dati personali proprio per la necessità di perseguire legittimi interessi. Il considerando in esame espressamente prevede anche che "*può essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto*".

2.5 Capo IV: titolare del trattamento e responsabile del trattamento

Se da un lato sono nettamente rafforzati i diritti dell'interessato, dall'altro sono maggiori anche gli oneri che gravano sul titolare e sul responsabile del trattamento: non a caso, dopo il Capo appena preso in esame, troviamo il Capo IV, dedicato interamente a queste due figure, le cui definizioni le possiamo individuare rispettivamente negli articoli 24 e 28 del Regolamento.

L'articolo 24, rubricato "responsabilità del titolare del trattamento", recita:

1. *Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del*

trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

2. *Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.*
3. *L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.*

L'articolo 28, invece, si riferisce al "responsabile del trattamento":

1. *Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.*
2. *Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.*
3. *I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione, o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali*

e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. […]

La prima disposizione del Capo in questione è l'articolo 24, il quale, al paragrafo 1, disciplina il principio di responsabilità o di *accountability*, già menzionato nell'articolo 5 paragrafo 2: il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate non solo per garantire, ma anche per dimostrare che il trattamento è effettuato nel rispetto del Regolamento. Tale concetto non è espressamente enunciato nella Direttiva 95/46/CE, ma lo è successivamente in altre fonti, come ad esempio nella Convenzione 108, dove la nozione di *accountability* viene introdotta dal "*Draft Protocol*".

Tra i vari principi sostanziali introdotti dal GDPR, l'*accountability* è oggi considerata come un approccio pratico alla *privacy* e al trattamento dei dati personali; essa punta, pertanto, allo sviluppo di strumenti che possano essere utilizzati dalle organizzazioni per valutare lo stato della propria *accountability* e renderne conto alle Autorità Garanti per la protezione dei dati personali. Una particolare applicazione di questo concetto è possibile rinvenirla in un settore dalle capacità espansive sostanzialmente illimitate: la sicurezza informatica. In questo settore, infatti, l'*accountability* può essere intesa come la capacità di un sistema di identificare un singolo utente e determinarne le azioni e il comportamento all'interno del sistema stesso grazie al supporto dell'audit delle tracce e di un sistema di autenticazione (*login*). L'uso di questo concetto, almeno in origine, non era tanto settorializzato e, anzi, veniva recepito ad un livello più generico come quello politico.

In generale si deve, però, ritenere che l'*accountability* rappresenti un aspetto del controllo di accesso che si basa sulla concezione che gli individui siano responsabili per le proprie azioni all'interno del sistema e che debbano, appunto, renderne conto ai terzi che ne facciano richiesta. In realtà il termine "*accountability*" richiama almeno due accezioni o componenti fondamentali:

- da un lato il dar conto all'esterno e in particolare al complesso degli *stakeholder* (delle parti interessate), in modo esaustivo e comprensibile, del corretto utilizzo delle risorse e della produzione di risultati in linea con gli scopi istituzionali;
- dall'altro, l'esigenza di introdurre logiche e meccanismi di maggiore responsabilizzazione interna alle aziende e alle reti di aziende relativamente all'impiego di tali risorse e alla produzione di correlati risultati.

L'*accountability* investe tutte le operazioni dell'azienda, anche se è nata specificatamente con riferimento alle informazioni economico-finanziarie e patrimoniali consuntive.

In ambito pubblicistico il concetto di *accountability* è sicuramente collegato a quello di trasparenza. Difatti le istituzioni pubbliche compiono, o non compiono, quotidianamente atti rilevanti per la comunità nazionale. Ma proprio una tale responsabilità, mette i cittadini nelle condizioni di formulare domande e osservazioni sul rendimento degli uffici pubblici e dei dirigenti che li guidano. I cittadini chiedono che il potere amministrativo adotti delle decisioni, ma, allo stesso tempo, chiedono che queste decisioni risolvano i loro problemi e che siano comprensibili e trasparenti. In altre parole, chiedono di "rendere conto".

L'*accountability* si compone di almeno tre elementi:

- La "trasparenza" intesa come garanzia della completa accessibilità alle informazioni, in primo luogo per i cittadini, anche in quanto utenti del servizio.
- La "responsività" intesa come la capacità di rendere conto di scelte, comportamenti e azioni e di rispondere alle questioni poste dagli stakeholder.
- La "compliance" intesa come capacità di far rispettare le norme, sia nel senso di finalizzare l'azione pubblica all'obiettivo stabilito nelle leggi, che nel senso di fare osservare le regole di comportamento degli operatori della pubblica amministrazione.

Il concetto in esame, dal punto di vista della privacy, non si risolve nella mera responsabilità, ma coinvolge aspetti quali l'affidabilità e la competenza aziendale nella gestione dei dati personali. Le fonti dell'*accountability* possono essere legislative, amministrative e contrattuali. Il titolare del trattamento deve essere in grado di dimostrare che ha adottato un processo complessivo di misure giuridiche, organizzative, tecniche, per la protezione di dati personali, anche attraverso l'elaborazione di specifici modelli organizzativi.

L'articolo 28, invece, introduce la figura del responsabile del trattamento, descrivendone caratteristiche e funzioni. Inoltre analizza il caso di cambiamento del responsabile del trattamento ed elenca tassativamente quali siano le previsioni del contratto o atto giuridico a egli riferito.

Il responsabile del trattamento è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento. Si tratta di un soggetto, distinto col titolare, che deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato. Il responsabile del trattamento dovrà avere innanzitutto una competenza qualificata, dovendo garantire una conoscenza specialistica della materia, e l'attuazione delle misure tecniche e organizzative in grado di soddisfare i requisiti stabiliti dal Regolamento europeo. Inoltre dovrà garantire particolare affidabilità, un requisito fondato su aspetti etici e deontologici, ad esempio l'assenza di condanne penali. Ovviamente dovrà disporre delle risorse tecniche adeguate per l'attuazione degli obblighi derivanti dal contratto di designazione e dalle norme in materia. Se è soggetto interno le risorse saranno a carico del titolare.

Gli articoli successivi, poi, sanciscono specifici adempimenti a cui questi due soggetti sono tenuti, in particolare:

- svolgere valutazioni d'impatto;
- notificare eventuali violazioni di dati;
- tenere registri circa le attività di trattamento;
- aderire a codici di condotta oppure a meccanismi di certificazione;

- designare un delegato alla protezione dei dati.

Passando all'analisi dei vari oneri che riguardano le due figure appena nominate, il Regolamento 2016/679 introduce due importantissimi principi, enunciati all'articolo 25, e riguardano soprattutto il titolare del trattamento. Comunemente si parla di "*privacy by design*" e "*privacy by default*", la cui traduzione in italiano è "protezione dei dati fin dalla progettazione e protezione per impostazione predefinita", che peraltro è proprio il contenuto della rubrica dell'articolo presente.

Il primo dei due principi è sancito dal paragrafo 1, il quale richiede che il titolare metta in atto misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati, non solo nella fase dell'esecuzione del trattamento, ma fin dal momento della progettazione dello stesso. Il secondo principio invece è affermato dal paragrafo 2 e sancisce che il titolare deve mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solamente i dati personali necessari per ciascuna specifica finalità del trattamento. Le misure in questione devono garantire in modo particolare che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone senza l'intervento umano. Va sottolineato che la protezione di "*default*" riguarda:

- la quantità dei dati raccolti;
- l'estensione del trattamento;
- il periodo di conservazione;
- l'accessibilità.

La portata di questi due principi non va affatto sottovalutata poiché, così facendo, si impone alle imprese (come d'altronde anche alle pubbliche amministrazioni) un approccio proattivo: la protezione dei dati contemporanea è un vero e proprio *asset* strategico, da valutare già nella fase di progettazione di nuove procedure, prodotti o servizi.

Proseguendo con l'analisi dei nuovi obblighi e responsabilità, l'articolo 30 riguarda i "registri delle attività di trattamento": il paragrafo 1 prevede che il titolare del trattamento debba tenere un registro delle attività svolte sotto la propria responsabilità, e in base al paragrafo 2 anche il responsabile del trattamento deve tenere un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare. I registri appena menzionati sono tenuti in forma scritta ed in formato elettronico. Tuttavia tale obbligo non si applica alle imprese o organizzazioni con meno di 250 dipendenti, con alcune eccezioni.

L'articolo 32, in materia di "sicurezza del trattamento", mantenendo una linea molto simile a quelli che lo precedono, impone sia al titolare che al responsabile del trattamento di porre in essere, tenendo in conto una serie di fattori, misure tecniche e organizzative idonee a garantire un livello di sicurezza del trattamento adeguato al rischio: il trattamento stesso potrebbe infatti esporre a rischi i diritti e le libertà degli individui nel caso in cui i dati personali venissero persi, modificati, divulgati senza autorizzazione, o dove si verificasse un accesso illecito ad essi. Tra queste misure, ad esempio, possiamo trovare quella della pseudonimizzazione e la cifratura dei dati, nonché la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico. Va ricordato che l'articolo 32 del Regolamento riprende l'articolo 17 della Direttiva 95/46/CE, ma dell'argomento in questione si occupano anche la Convenzione 108 e varie risoluzioni del 1973-1974.

Tuttavia, nonostante simili misure, potrebbe comunque verificarsi una violazione: si parla, in questo caso, di "*data breach*" (violazione dei dati), ed è qui che sta la vera novità. In tale situazione, infatti, due sono gli obblighi da adempiere: la notifica della violazione all'autorità di controllo (articolo 33) e, in alcuni casi, la comunicazione al diretto interessato (articolo 34).

L'articolo 33 prevede che il responsabile del trattamento, dopo essere venuto a conoscenza della violazione, debba informare il titolare del trattamento senza ingiustificato ritardo. A quel punto il titolare deve notificare la violazione all'autorità di controllo competente, a sua volta senza giustificato ritardo e ove

possibile entro 72 ore dal momento in cui ne è venuto a conoscenza; se invece la notifica non sia effettuata entro 72 ore, deve essere corredata da una motivata giustificazione del ritardo. Questo obbligo viene meno nel caso in cui sia improbabile che la violazione presenti un rischio per i diritti e le libertà degli individui. Lo scopo dell'articolo in questione è chiaramente quello di permettere all'autorità di controllo di agire prontamente, valutando la gravità di tale "*data breach"* e quali misure imporre al titolare.

L'articolo 34, poi, pone in capo al titolare del trattamento un dovere di comunicazione anche nei confronti dell'interessato, ma ciò solo se la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone. Inoltre la suddetta comunicazione non è richiesta anche nei casi del paragrafo 3, cioè quando il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione; quando il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati; e infine quando detta comunicazione richiederebbe sforzi sproporzionati, ed in tal caso si procede a una comunicazione pubblica o a una misura simile.

Da sottolineare che l'articolo 33, in relazione all'obbligo di notifica all'autorità di controllo, fa riferimento a un "rischio per i diritti e le libertà"; l'articolo 34, invece, affinché scatti l'obbligo di comunicazione all'interessato, richiede che il rischio sia "elevato", cioè una soglia di pericolo maggiore. Questo sia per ridurre gli oneri, sia per evitare allarmismi inutili da parte degli individui in presenza di violazioni non particolarmente significative.

Un'altra disposizione importante riguardante oneri appartenenti a titolare e responsabile del trattamento è l'articolo 35, il quale parla delle "valutazioni d'impatto", che rappresentano una novità di particolare rilievo nell'ambito del Regolamento 2016/679. Il primo paragrafo prevede che, qualora un certo tipo di trattamento, in ragione dell'utilizzo di nuove tecnologie, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento stesso, possa presentare

un rischio elevato per i diritti e le libertà delle persone interessate, il titolare debba effettuare una valutazione dell'impatto potenziale delle operazioni preventivate. Il paragrafo 3, poi, elenca alcuni casi in cui la suddetta analisi è richiesta in modo particolare, ad esempio quando siamo in presenza di "*una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche*" oppure quando ci troviamo di fronte al "*trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1*" (cioè i "dati sensibili" a cui si è fatto riferimento precedentemente). È però il paragrafo 7 che specifica quale debba essere il contenuto minimo della valutazione d'impatto, ovvero:

- una descrizione dei trattamenti previsti e delle finalità del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per diritti e libertà delle persone interessate;
- le misure e i meccanismi per garantire la protezione dei dati e dimostrare la conformità al Regolamento.

Fondamentale è poi il ruolo che l'articolo 35 attribuisce all'autorità di controllo nazionale: essa deve redigere e rendere pubblico un elenco delle tipologie di trattamento soggette alla valutazione d'impatto; inoltre può fare lo stesso anche con le tipologie di trattamento che, al contrario, non sono soggette a tale requisito. Tali elenchi devono essere comunicati al Comitato europeo per la protezione dei dati previsto dall'articolo 68. Ma l'autorità di controllo svolge anche un'attività consultiva di tipo preventivo, disciplinata dall'articolo 36 del Regolamento: infatti il titolare, prima di procedere al trattamento, consulta l'autorità qualora la valutazione d'impatto indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare per attenuare il rischio; e, se ritiene che il trattamento in questione violi il Regolamento, specialmente qualora il titolare non

abbia identificato o attenuato il rischio a sufficienza, l'autorità fornisce un parere scritto e può avvalersi dei poteri di indagine e correttivi previsti dall'articolo 58.

2.5.1 *Data Protection Officer*

Per concludere l'analisi degli obblighi del titolare e del responsabile del trattamento, è opportuno soffermarsi con particolare attenzione su quella che è senza dubbio la più importante figura soggettiva introdotta dal Regolamento 2016/679: il responsabile della protezione dei dati (RPD), o *Data Protection Officer* (DPO), disciplinato dagli articoli 37, 38 e 39. Infatti il titolare e il responsabile del trattamento, sulla base dell'articolo 37 paragrafo 1, devono designare un DPO quando:

- il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico (eccetto le autorità giurisdizionali nell'esercizio di funzioni giurisdizionali);
- le attività principali del titolare o del responsabile consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- il titolare o il responsabile trattano dati sensibili o dati giudiziari.

Si tratta ovviamente di casi in cui si ritiene che il trattamento presenti rischi specifici. Le società che fanno parte di uno stesso gruppo imprenditoriale, a livello nazionale o transfrontaliero, possono nominare un unico DPO, a patto che sia facilmente raggiungibile da ciascuno stabilimento. Qualcosa di simile a quanto appena affermato è previsto anche per i soggetti pubblici: è infatti possibile designare un solo DPO per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e della loro dimensione.

Il DPO deve essere in possesso di specifici requisiti professionali, tra cui soprattutto la conoscenza delle norme e delle prassi in materia di protezione dei dati, e la capacità di assolvere i compiti dell'articolo 39. Inoltre il DPO:

- deve essere indipendente: il titolare e il responsabile del trattamento, infatti, si assicurano che il DPO non riceva alcuna istruzione per quanto riguarda lo svolgimento delle sue funzioni;
- deve mantenere il segreto e la riservatezza in merito all'adempimento dei propri compiti;
- può svolgere altri compiti e funzioni, ma senza che essi diano adito a un conflitto di interessi (cosa di cui si assicura il titolare o il responsabile del trattamento).

Come appena detto, è necessario che il titolare o il responsabile si assicurino che determinati compiti o funzioni non determinino conflitti di interesse, quali ad esempio:

- conflitto di interesse correlato all'assunzione da parte del DPO di ruoli dirigenziali impattanti la gestione dei dati personali; tale tipologia di conflitto potrebbe essere accentuata nel caso in cui, nell'esercizio dei propri compiti e funzioni, il DPO debba indicare, suggerire o raccomandare, nell'ambito della struttura organizzativa di cui è responsabile, interventi specifici che impattano il trattamento dei dati personali, ad esempio, il responsabile della funzione IT, che riveste anche il ruolo di DPO potrebbe indicare, suggerire o raccomandare un'applicazione o una misura procedurale e/o tecnologica conveniente ai suoi scopi, ma meno conforme alla normativa.

In aggiunta all'esempio di conflitto di interesse appena citato, che tra l'altro è l'unico espressamente previsto dalla norma in questione, se ne possono rinvenire altri grazie all'analisi compiuta da diversi giuristi:

- conflitto d'interesse correlato al tempo impiegato nell'adempimento alle mansioni di DPO e quello dedicato ad altri compiti e funzioni; tale tipologia di conflitto potrebbe essere accentuata nel caso in cui la valutazione del DPO tenga maggiormente conto delle mansioni e non del suo operato come tale nonché all'avvio di nuove attività cogenti richieste dal Regolamento stesso (ad esempio, valutazione d'impatto sulla protezione dei dati, registro dei trattamenti). Pertanto è opportuno che il DPO, per la stessa natura del ruolo e responsabilità che investe, non si trovi mai nella posizione di dover sottrarre tempo ai propri adempimenti a favore di altri compiti e funzioni;
- conflitto di interesse legato alla posizione gerarchica del personale impiegato nel supporto alle attività del DPO e nello svolgimento di altri compiti e funzioni; tale tipologia di conflitto potrebbe essere accentuato nel caso in cui, ad esempio, una risorsa della funzione IT[87], che collabora anche con il DPO, debba fornire raccomandazioni rispetto all'applicazione di una misura procedurale e/o tecnologica al responsabile della struttura organizzativa di appartenenza;

Va ricordato che il DPO può essere un dipendente del titolare o del responsabile del trattamento, o in alternativa può svolgere i propri compiti sulla base di un contratto di servizi; in ogni caso, i dati del DPO dovranno essere resi pubblici, nonché comunicati all'autorità di controllo.

Veniamo ora, nello specifico, alle funzioni che il Regolamento attribuisce al responsabile della protezione dei dati. Il DPO, che deve essere "*tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali*", è incaricato dello svolgimento dei compiti dell'articolo 39 paragrafo 1:

[87] L'*IT service management* (o gestione dei servizi IT, abbreviato in *ITSM*) è una disciplina che si occupa di pianificare, progettare e gestire i sistemi di *information technology* (IT) di un'organizzazione.

- "*informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;*
- *sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;*
- *fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;*
- *cooperare con l'autorità di controllo; e*
- *fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione*".

Ma le due disposizioni che, meglio delle altre, ci permettono di capire la caratura di questa nuova figura soggettiva, almeno nelle intenzioni del legislatore europeo, sono rispettivamente l'articolo 38 paragrafo 4 e ancor di più l'articolo 38 paragrafo 3 ultimo periodo. In base alla prima di tali disposizioni, "*gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento*"; il DPO costituisce quindi un fondamentale punto di contatto e un importante riferimento per tutti i cittadini i cui dati sono trattati. L'articolo 38 paragrafo 3 ultimo periodo, infine, recita: "*il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento*". Ciò significa che il DPO si

interfaccerà direttamente con l'amministratore delegato o comunque con i vertici gerarchici della società, senza passaggi intermedi. Siamo dunque di fronte a un soggetto autonomo e indipendente che nell'organizzazione aziendale avrà un grande spessore.

2.5.2 Codici di condotta e certificazione

Ultimata una descrizione generale sul DPO, meritano una menzione anche i codici di condotta. Ad essi faceva riferimento già la Direttiva 95/46/CE all'articolo 27, ma l'articolo 40 del Regolamento 2016/679 è ben più dettagliato. Il paragrafo 1 del presente articolo prevede che " *gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese*". A elaborare, modificare o prorogare tali codici allo scopo di precisare l'applicazione del Regolamento sono le associazioni e gli altri organismi rappresentanti le categorie di titolari o responsabili del trattamento. I progetti di codice, come le modifiche e le proroghe, sono sottoposti all'autorità di controllo che esprime un parere sulla conformità al Regolamento e infine approva, se ritiene che siano offerte in misura sufficiente, garanzie adeguate. Inoltre, a certe condizioni, la Commissione può decidere mediante atti di esecuzione che determinati codici di condotta a lei sottoposti abbiano validità generale all'interno dell'Unione, e lo stesso vale per le modifiche e le proroghe.

Un cenno va fatto agli articoli 41, 42 e 43. Il primo dei tre disciplina il meccanismo di "monitoraggio dei codici di condotta", ma la vera novità è quella prevista dall'articolo 42, il quale parla dei meccanismi di "certificazione". Secondo il paragrafo 1 di tale articolo " *gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione,*

l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese". Tale certificazione, che è volontaria e accessibile tramite una procedura trasparente, prevista al paragrafo 5 del medesimo articolo, viene rilasciata da appositi organismi disciplinati all'articolo 43 o dall'autorità di controllo per un periodo massimo di tre anni, e può essere rinnovata, ma anche revocata, prima della scadenza. Da sottolineare, però, che la certificazione non riduce la responsabilità del titolare e del responsabile del trattamento riguardo alla conformità al Regolamento e lascia impregiudicati compiti e poteri dell'autorità di controllo.

2.6 Capo V: trasferimenti di dati personali

Ultimata la trattazione delle disposizioni del Capo IV si può passare al contenuto del Capo V, il quale riguarda il "trasferimento dei dati personali verso paesi terzi o organizzazioni internazionali" e comprende gli articoli da 44 a 50 del Regolamento. Occorre precisare che il Regolamento 2016/679 lascia fondamentalmente invariata l'impostazione già sancita dalla Direttiva 95/46/CE, in particolar modo nei suoi articoli 25 e 26.

La norma principale del Capo V del Regolamento è l'articolo 44, il quale detta il "principio generale per il trasferimento", e recita: "*qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte*

salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato".

Prima di analizzare le disposizioni successive all'ultima citata, bisogna fare un piccolo accenno all'articolo 25 della Direttiva del 1995, il quale assicura la possibilità di trasferire i dati verso Stati che si trovano fuori dall'UE, purché questi garantiscano un livello di protezione adeguato. Nel valutare l'adeguatezza, bisogna prendere in considerazione in particolare "*la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate*". Inoltre gli Stati membri e la Commissione si comunicano vicendevolmente i casi in cui, a loro parere, un paese terzo non garantisce un adeguato livello di protezione. E, qualora la Commissione comprenda che uno stato extraeuropeo non garantisce un adeguato livello di protezione, i paesi UE devono adottare ogni misura necessaria per impedire i trasferimenti di dati verso quello Stato.

Come già detto, le disposizioni del Regolamento 679 che riguardano i trasferimenti non appaiono particolarmente innovative, ma sicuramente la disciplina nuova risulta più completa e dettagliata. L'articolo 45, rubricato "trasferimento sulla base di una decisione di adeguatezza", in particolar modo nel suo paragrafo 2, elenca in modo più preciso rispetto all'articolo 25 della Direttiva quali sono i criteri che devono guidare la valutazione di adeguatezza del livello di protezione garantito dal paese terzo o dall'organizzazione internazionale; a titolo esemplificativo, troviamo:

- lo stato di diritto;
- il rispetto dei diritti umani e delle libertà fondamentali;
- la pertinente legislazione generale e settoriale;
- l'attuazione di tale legislazione;
- la giurisprudenza;
- un ricorso effettivo in sede amministrativa e giudiziaria;

- l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti;
- gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale;
- la loro partecipazione a sistemi multilaterali o regionali.

La decisione di adeguatezza, che viene presa dalla Commissione mediante atti di esecuzione, è sottoposta ad un riesame periodico, almeno ogni quattro anni, che tenga conto di tutti gli sviluppi. Inoltre, ove si ravvisi la necessità, la Commissione può revocare, modificare o sospendere la decisione di adeguatezza.

Cosa accade nel caso in cui la decisione di adeguatezza manchi? Il trasferimento può essere comunque effettuato, ma a determinate condizioni. L'articolo 46, in materia, rubricato "trasferimento soggetto a garanzie adeguate", nel suo paragrafo 1, prevede che il titolare o il responsabile del trattamento possa "*trasferire dati personali verso un paese terzo o un'organizzazione internazionale sole se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi*". Quali siano queste garanzie adeguate ci viene detto dal paragrafo 2 del medesimo articolo, in particolar modo:

- norme vincolanti d'impresa;
- clausole contrattuali tipo;
- codici di condotta;
- meccanismi di certificazione approvati.

La disposizione in questione ha come sua disposizione ispiratrice l'articolo 26 paragrafo 2 della Direttiva 95/46/CE, che a sua differenza usa l'espressione "garanzie sufficienti".

Altra disposizione importante è l'articolo 49, il quale contiene "deroghe in specifiche situazioni", le quali consentono il trasferimento pur mancando sia la decisione di adeguatezza dell'articolo 45, che le garanzie adeguate dell'articolo 46. Ma neppure tale disposizione rappresenta una novità, poiché il suo contenuto

è praticamente identico a quello dell'articolo 26 paragrafo 1 della Direttiva 95/46/CE. Tra queste deroghe, comunque, figurano i casi in cui:

- l'interessato ha acconsentito esplicitamente al trasferimento proposto;
- il trasferimento sia necessario all'esecuzione di un contratto concluso tra interessato e titolare del trattamento;
- il trasferimento sia necessario per la conclusione di un contratto stipulato tra titolare del trattamento e altra persona fisica o giuridica;
- il trasferimento è necessario per importanti motivi di interesse pubblico;
- il trasferimento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
- il trasferimento è necessario per tutelare gli interessi vitali dell'interessato o di altre persone;
- il trasferimento è effettuato a partire da un registro che mira a fornire informazioni al pubblico e può essere consultato tanto dal pubblico che da chiunque abbia un legittimo interesse.

La norma di chiusura del Capo V è l'articolo 50, rubricato "cooperazione internazionale per la protezione dei dati personali", la cui importanza impone di citarlo testualmente per intero:

1. *In relazione ai paesi terzi e alle organizzazioni internazionali, la Commissione e le autorità di controllo adottano misure appropriate per:*

- *sviluppare meccanismi di cooperazione internazionale per facilitare l'applicazione efficace della legislazione sulla protezione dei dati personali;*
- *prestare assistenza reciproca a livello internazionale nell'applicazione della legislazione sulla protezione dei dati personali, in particolare mediante notificazione, deferimento dei reclami, assistenza alle indagini e scambio di informazioni, fatte salve garanzie adeguate per la protezione dei dati personali e gli altri diritti e libertà fondamentali;*

- *coinvolgere le parti interessate pertinenti in discussioni e attività dirette a promuovere la cooperazione internazionale nell'applicazione della legislazione sulla protezione dei dati personali;*
- *promuovere lo scambio e la documentazione delle legislazioni e prassi in materia di protezione dei dati personali, compresi i conflitti di giurisdizione con paesi terzi.*

2.7 Capo VI: autorità di controllo indipendenti

L'analisi si sposta adesso al Capo VI, che comprende gli articoli da 51 a 59, e riguarda le "autorità di controllo indipendenti" (*Data Protection Authority*, DPA), a cui già la Direttiva 46 del 1995 dedicava l'articolo 28. Inoltre il presente Capo è diviso in due sezioni: la sezione 1 riguarda l'indipendenza, e comprende gli articoli da 51 a 54; la sezione 2 riguarda la competenza, i compiti e i poteri, e comprende gli articoli da 55 a 59.

La prima sezione è dedicata alla definizione di "autorità di controllo" (art. 51), alle "condizioni di indipendenza" (art. 52), alla "nomina dei membri" (art. 53) e alle "norme sull'istituzione dell'autorità di controllo" (art. 54). L'articolo principale di questa sezione è dunque il 51, il quale stabilisce che:

1. *Ogni stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione del presente regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare le libera circolazione dei dati personali all'interno dell'Unione ("l'autorità di controllo").*
2. *Ogni autorità di controllo contribuisce alla coerente applicazione del presente regolamento in tutta l'Unione. A tale scopo, le autorità di controllo cooperano tra loro e con la Commissione, conformemente al capo VII.*

3. *Qualora in uno Stato membro siano istituite più autorità di controllo, detto Stato membro designa l'autorità di controllo che rappresenta tali autorità nel comitato e stabilisce il meccanismo in base al quale le altre autorità si conformano alle norme relative al meccanismo di coerenza di cui all'articolo 63.* […]

L'articolo appena citato non necessita di ulteriori approfondimenti, vista la sua chiarezza e analiticità, come d'altronde l'articolo seguente, il 52, che prevede le "condizioni di indipendenza":

1. *Ogni autorità di controllo agisce in piena indipendenza nell'adempimento dei propri compiti e nell'esercizio dei propri poteri conformemente al presente regolamento.*
2. *Nell'adempimento dei rispettivi compiti e nell'esercizio dei rispettivi poteri previsti dal presente regolamento, il membro o i membri di ogni autorità di controllo non subiscono pressioni esterne, né dirette, né indirette, e non sollecitano né accettano istruzioni da alcuno.*
3. *Il membro o i membri dell'autorità di controllo si astengono da qualunque azione incompatibile con le loro funzioni e per tutta la durata del mandato non possono esercitare alcuna altra attività incompatibile, remunerata o meno.*
4. *Ogni Stato membro provvede affinché ogni autorità di controllo sia dotata delle risorse umane, tecniche e finanziarie, dei locali e delle infrastrutture necessari per l'effettivo adempimento dei suoi compiti e l'esercizio dei propri poteri, compresi quelli nell'ambito dell'assistenza reciproca, della cooperazione e della partecipazione al comitato.*
5. *Ogni Stato membro provvede affinché ogni autorità di controllo selezioni e disponga di proprio personale, soggetto alla direzione esclusiva del membro o dei membri dell'autorità di controllo interessata.*
6. *Ogni Stato membro provvede affinché ogni autorità di controllo sia soggetta a un controllo finanziario che non ne pregiudichi l'indipendenza*

e disponga di bilanci annuali, separati e pubblici, che possono far parte del bilancio generale statale o nazionale.

La sezione 1 si conclude con le previsioni sulla nomina dei membri e sull'istituzione dell'autorità, come anticipato precedentemente.

2.7.1 Competenza, compiti e poteri

Nell'ambito della seconda sezione che descrive la competenza (art. 55), i compiti (art. 57) e i poteri (art. 58) delle autorità garanti, interessanti innovazioni sono rappresentate dalla figura dell'autorità capofila (art. 56) e del criterio territoriale per la sua competenza.

L'articolo 55 apre la sezione 2 del capo presente e parla della competenza in questi termini:

1. *Ogni autorità di controllo è competente a eseguire i compiti assegnati e a esercitare i poteri a essa conferiti a norma del presente regolamento nel territorio del rispettivo Stato membro.*
2. *Se il trattamento è effettuato da autorità pubbliche o organismi privati che agiscono sulla base dell'articolo 6, paragrafo 1, lettera c) o e), è competente l'autorità di controllo dello Stato membro interessato. In tal caso, non si applica l'articolo 56.*
3. *Le autorità di controllo non sono competenti per il controllo dei trattamenti effettuati dalle autorità giurisdizionali nell'esercizio delle loro funzioni giurisdizionali.*

Al paragrafo 1 è rinvenibile il principio di territorialità della competenza sancito dal regolamento, mentre nei due paragrafi successivi sono concepiti casi specifici.

Prima di analizzare la figura dell'autorità capofila prevista dall'articolo 56, però, è opportuno fare un piccolo riferimento alle disposizioni previste dagli articoli 57 e 58, due articoli "monumentali" se si guarda alla loro lunghezza. Basti pensare che solo nell'individuazione dei compiti il legislatore utilizza nell'elenco le lettere dalla a) fino alla v).

L'articolo 57 enuclea una serie molto ampia di compiti che spettano ad un'autorità di controllo sul proprio territorio, tra cui rientrano il dovere di:

- sorvegliare sulla corretta applicazione del regolamento (lett. a);
- promuovere la conoscenza, la consapevolezza e la comprensione verso il pubblico dei rischi, delle dinamiche e delle garanzie relative alla protezione dei dati personali (lett. b);
- compito di svolgere funzione di consulenza per parlamenti, governi o istituzioni nazionali (lett.c);
- promuovere la consapevolezza dei titolari del trattamento riguardo ai loro obblighi e doveri (lett. d);
- trattare i reclami proposti da un interessato (lett. f);
- collaborare con altre autorità mediante scambio di informazioni (lett. g);
- svolge qualsiasi altro compito legato alla protezione dei dati personali (lett. v).

L'articolo 58 del Regolamento, invece, riconosce in capo ad ogni autorità la possibilità di esercitare tre gruppi di poteri:

1. Il primo gruppo è composto dai poteri di indagine tra cui rientrano: la facoltà di ingiungere al titolare di fornirgli ogni tipo di informazione, consentirgli l'accesso ai dati e ai locali se necessario allo svolgimento dei suoi compiti, oppure la possibilità di svolgere attività di indagine sotto forma di revisione sulla protezione dei dati, di effettuare riesami delle certificazioni rilasciate e infine di notificare al titolare e al responsabile le presunte violazioni delle disposizioni regolamentari.

2. Il secondo gruppo invece è costituito da poteri correttivi che si esplicano nella facoltà per l'autorità garante di: rivolgere ammonimenti al titolare o al responsabile del trattamento quando il trattamento possa violare o abbia violato le disposizioni del regolamento; ingiungere al titolare di soddisfare le richieste dell'interessato all'esercizio dei propri diritti, di conformare il trattamento, comunicare all'interessato l'avvenuta violazione dei dati personali, di limitare temporaneamente o definitivamente il trattamento, di rettificare o cancellare i dati personali, la sospensione dei flussi di dati verso un destinatario in un paese terzo.
3. Infine il terzo gruppo prevede poteri autorizzativi e consultivi nel caso in cui all'autorità sia richiesto di: fornire consulenza al titolare secondo la procedura di consultazione preventiva, rilasciare pareri destinati ai parlamenti, ai governi, ad altri organismi e istituzioni nazionali nonché al pubblico su questioni riguardanti la protezione dei dati personali; rilasciare certificazioni e approvarne i criteri, adottare le clausole tipo di protezione dei dati e infine approvare le norme vincolanti d'impresa.

In chiusura di disposizione è previsto, al paragrafo 4, il principio generale per cui l'esercizio dei poteri di un'autorità di controllo è soggetto a garanzie adeguate quali la possibilità di un ricorso giurisdizionale effettivo e il giusto processo, mentre, al paragrafo 5, si prevede che ogni Stato membro debba disporre per legge il potere per l'autorità di controllo d'intentare un'azione giudiziale o stragiudiziale qualora sia violato il Regolamento.

2.7.2 Autorità capofila

Come detto in precedenza, nello scenario predisposto dal Regolamento si inserisce una figura del tutto nuova, rappresentata dalla c.d. autorità di controllo

capofila. Al fine dell'individuazione della competenza di tale figura è fondamentale il criterio del c.d. meccanismo *one stop shop* o dello "sportello unico". Questo meccanismo, a carattere territoriale, opera solo ed esclusivamente per quanto riguarda i trattamenti di dati transfrontalieri in base a due presupposti: il primo statico, che rileva in base al numero di stabilimenti del titolare; il secondo dinamico, in base alle attività di trattamento effettive esercitate al di fuori dei confini nazionali che comportino dei riflessi giuridici sostanziali in capo a soggetti che risiedano in più Stati membri. Infatti la disposizione di cui all'articolo 56 intitolata "competenza dell'autorità di controllo capofila" dispone che "*l'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare e del trattamento o responsabile del trattamento è competente ad agire in qualità di autorità di controllo capofila per i trattamenti transfrontalieri effettuati dal suddetto titolare*".

L'autorità capofila gestisce i reclami ed è competente per le eventuali violazioni del Regolamento: in questo modo si impedisce che le violazioni delle medesime norme siano oggetto di ricorsi decisi in modo diverso dalle autorità di controllo dei vari Stati in cui il titolare opera. Dunque, la decisione dell'autorità capofila avrà efficacia vincolante anche per quanto riguarda i trattamenti effettuati da quello stesso titolare in altri paesi UE. In sintesi, all'autorità capofila competono compiti di cooperazione con le altre autorità di controllo coinvolte[88] anche se, ai sensi del paragrafo 6, solo la capofila unicamente riveste il ruolo di interlocutore del titolare e/o del responsabile, in merito al trattamento transfrontaliero.

[88] Le altre autorità di controllo sono coinvolte in quanto interessate per la presenza di filiali del responsabile del trattamento o per il coinvolgimento nelle operazioni di trattamento anche di propri cittadini, nonché, da ultimo, per aver ricevuto un reclamo avverso detto operatore.

2.8 Capo VII: cooperazione e coerenza

L'autorità di controllo capofila assume un ruolo di rilevante importanza anche nel Capo VII del Regolamento 2016/679, che si occupa di disciplinare la "cooperazione e coerenza", e comprende gli articoli da 60 a 76. Il presente Capo è composto da tre sezioni: la prima riguarda la cooperazione, la seconda la coerenza e la terza la figura del Comitato europeo per la protezione dei dati.

Le modalità di "cooperazione tra l'autorità di controllo capofila e le altre autorità di controllo interessate" sono descritte dall'articolo 60, il primo del Capo oggetto dell'attuale analisi, in cui è riportato l'iter decisionale da seguire[89]. È previsto un meccanismo di cooperazione per cui tutte le autorità coinvolte guidate dalla capofila, congiuntamente possono condurre operazioni di indagine, controllo e accertamento nei confronti del titolare del trattamento al fine di raggiungere un consenso. In tal senso è previsto che l'autorità capofila comunichi le informazioni sulla questione alle altre autorità, senza indugio, insieme ad un progetto di decisione. Successivamente le altre autorità di controllo redigono pareri motivati sulla proposta trasmessa dall'autorità capofila che nonostante non abbiano natura vincolante, devono essere presi in dovuta considerazione. Infatti, ispirata al principio di leale collaborazione, al fine di cementare la cooperazione e non svilire, rendendo poi in fin dei conti inutile il supporto delle altre autorità, si ritiene che l'autorità capofila non possa adottare un parere diverso. Qualora una delle autorità di controllo proponga un'obiezione in merito al progetto di decisione (entro un termine di quattro settimane da quando è stata consultata), qualora la capofila ritenga l'obiezione pertinente, redige un nuovo progetto da sottoporre al vaglio delle altre autorità entro un termine di due settimane; altrimenti, ove non ritenga l'obiezione pertinente o non motivata, sottopone la questione al "meccanismo di coerenza" previsto all'articolo 63 del Regolamento. Se nessuna obiezione è presentata, il progetto di decisione della capofila si ritiene accettato e vincolante

[89] Riferimenti importanti sono presenti in materia anche nei Considerando 125 e 126 del Regolamento UE 2016/679.

per tutte le autorità che vi hanno partecipato, di conseguenza l'autorità capofila "*adotta la decisione e la notifica allo stabilimento principale o allo stabilimento unico del titolare del trattamento o responsabile del trattamento, a seconda dei casi, e informa le altre autorità di controllo interessate e il comitato la decisione in questione, compresa una sintesi dei fatti e delle motivazioni pertinenti. L'autorità di controllo cui è stato proposto un reclamo informa il reclamante riguardo alla decisione*"[90].

La seconda sezione del capo VII si apre con l'articolo 63, il quale porta la rubrica "meccanismo di coerenza" e recita: "*al fine di contribuire all'applicazione coerente del presente regolamento in tutta l'Unione, le autorità di controllo cooperano tra loro e, se del caso, con la Commissione mediante il meccanismo di coerenza stabilito nella presente sezione*". Tale disposizione, quindi, va integrata con le disposizioni che la succedono:

- parere del comitato europeo per la protezione dei dati (articolo 64);
- composizione delle controversie da parte del comitato (articolo 65);
- procedura d'urgenza (articolo 66);
- scambio di informazioni (articolo 67).

2.8.1 Comitato europeo per la protezione dei dati

L'intera terza sezione del presente capo riguarda un'importante novità costituita dall'introduzione del Comitato europeo per la protezione dei dati personali. Anche in questo caso il legislatore non risparmia accuratezza e specificità nel definire in dettaglio composizione, indipendenza e compiti. Vista l'importanza di tale organo, previsto dall'articolo 68 del Regolamento, è opportuno citare per intero il testo della disposizione:

[90] Articolo 60, paragrafo 7, Regolamento UE 2016/679.

1. "*Il comitato europeo per la protezione dei dati ("comitato") è istituito quale organismo dell'Unione ed è dotato di personalità giuridica.*
2. *Il comitato è rappresentato dal suo presidente.*
3. *Il comitato è composto dalla figura di vertice di un'autorità di controllo per ciascuno Stato membro e dal garante europeo della protezione dei dati, o dai rispettivi rappresentanti.*
4. *Qualora, in uno Stato membro, più autorità di controllo siano incaricate di sorvegliare l'applicazione delle disposizioni del presente regolamento, è designato un rappresentante comune conformemente al diritto di tale Stato membro.*
5. *La Commissione ha il diritto di partecipare alle attività e alle riunioni del comitato senza diritto di voto. La Commissione designa un rappresentante. Il presidente del comitato comunica alla Commissione le attività del comitato.*
6. *Nei casi di cui all'articolo 65, il garante europeo della protezione dei dati ha diritto di voto solo per decisioni che riguardano principi e norme applicabili a istituzioni, organi, uffici e agenzie dell'Unione che corrispondono nella sostanza a quelli del presente regolamento*".

Il Comitato opera in piena indipendenza nell'esecuzione dei suoi compiti e nell'esercizio dei suoi poteri come previsto generalmente per ogni autorità garante indipendente, come stabilito dall'articolo 69.

All'articolo 70, invece, sono previsti i numerosi compiti del Comitato[91], il cui obiettivo principale è quello di garantire l'applicazione coerente del Regolamento tramite la pubblicazione di linee guida, raccomandazioni, pareri e migliori prassi, oppure tramite l'esame di propria iniziativa o su richiesta di uno dei suoi membri di qualsiasi questione relativa alla protezione dei dati personali e in merito alla interpretazione e applicazione corretta del Regolamento. Inoltre

[91] Nel paragrafo 1 dell'articolo 70 sono utilizzate le lettere dalla a) alla y), a testimonianza di quanti compiti abbia il Comitato.

svolge una funzione di consulenza per la Commissione in merito ai formati e alle procedure per lo scambio di informazioni tra titolari del trattamento e autorità di controllo, oppure per valutare l'adeguatezza del livello di protezione di un paese terzo o di un'organizzazione internazionale. Inoltre un compito molto importante del Comitato è rappresentato dall'opera di promozione nell'ambito della cooperazione e dell'assistenza reciproca tra autorità di controllo dove è previsto che il Comitato agevoli e implementi lo scambio di informazioni e prassi, di programmi comuni di formazione e di personale, nonché di conoscenze e documentazione sulla legislazione in tema di protezione dei dati personali tra autorità di controllo europee, ma anche di tutto il mondo.

Il Comitato inoltre:

- redige una relazione annuale sulla protezione dei dati che poi viene pubblicata e trasmessa al Parlamento europeo, al Consiglio e alla Commissione (articolo 71);
- decide a maggioranza semplice, salvo diversamente previsto, e si dota di un proprio regolamento interno (articolo 72);
- elegge un presidente e due vicepresidenti, con mandato quinquennale, rinnovabile una volta (articolo 73). Il presidente ha compiti di convocazione, notificazione ed esecuzione (articolo 74);
- dispone di una segreteria messa a disposizione dal garante europeo della protezione dei dati e svolge i propri compiti seguendo esclusivamente le istruzioni del presidente del comitato. La segreteria presta assistenza in materia di analisi, amministrativa e logistica al comitato (articolo 75);
- può deliberare con carattere di riservatezza (articolo 76).

2.9 Capo VIII: mezzi di ricorso, responsabilità e sanzioni

Il Capo VIII del Regolamento 2016/679 tratta i mezzi di ricorso, le responsabilità e le sanzioni.

Per quanto riguarda i mezzi di ricorso, il primo che salta all'occhio è sicuramente il reclamo, previsto nell'articolo 77, che disciplina il diritto di proporre reclamo all'autorità di controllo da parte dell'interessato o del suo rappresentante. Nei successivi articoli 78 e 79 sono invece rispettivamente sanciti il diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo e il diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento. L'articolo 77, inoltre, sottolinea che il reclamo va presentano nello Stato membro in cui risiede abitualmente, lavora oppure nel luogo ove si è verificata la presunta violazione

L'articolo 80 disciplina la rappresentanza degli interessati, fondamentale anche in riferimento a quanto detto precedentemente sulla possibilità che sia anche il rappresentante dell'interessato a proporre reclamo nei confronti di un'autorità di controllo, e afferma che:

1. "*L'interessato ha il diritto di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro, che siano debitamente costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di proporre il reclamo per suo conto e di esercitare per suo conto i diritti di cui agli articoli 77, 78 e 79 nonché, se previsto dal diritto degli Stati membri, il diritto di ottenere il risarcimento di cui all'articolo 82.*
2. *Gli Stati membri possono prevedere che un organismo, organizzazione o associazione di cui al paragrafo 1 del presente articolo, indipendentemente dal mandato conferito dall'interessato, abbia il diritto di proporre, in tale Stato membro, un reclamo all'autorità di controllo competente, e di*

esercitare i diritti di cui agli articoli 78 e 79, qualora ritenga che i diritti di cui un interessato gode a norma del presente regolamento siano stati violati in seguito al trattamento".

Affrontati i temi del reclamo e della rappresentanza, sicuramente il maggiore cambio di prospettiva adottato dal Regolamento è quello di aver incentrato il nuovo sistema interamente sulle figure del *Controller* (titolare) e del *Processor* (responsabile) e sui profili degli obblighi e dei doveri di questi ultimi, connessi al rispetto delle norme giuridiche e tecniche del trattamento dei dati personali. La disciplina, dunque, non è più incentrata esclusivamente sui diritti dell'interessato, quali perno fondamentale del diritto alla protezione dei dati, ma la tutela, in un'ottica dichiaratamente preventiva e di tipo precauzionale, passa necessariamente attraverso un'attenta elaborazione di ogni fase del trattamento dei dati (specialmente delle misure di sicurezza) prima che venga posta in essere. La tutela, inoltre, passa anche attraverso la definizione puntuale degli obblighi e dei doveri dei principali soggetti che partecipano al procedimento (Titolare e Responsabile), in ossequio al principio di responsabilizzazione (*accountability*) previsto all'articolo 5, paragrafo 2 del Regolamento. Il regime di responsabilità civile elaborato dal Regolamento del 2016, è tutt'altro che agevole per il titolare e il responsabile del trattamento che, a norma dell'articolo 82[92], rispondono per qualsiasi danno materiale o immateriale causato da una violazione del Regolamento stesso seguendo, all'accertamento di tale violazione, il diritto al

[92] La ripartizione della responsabilità prevista dall'articolo 82, paragrafo 2, segue un modello a cascata per il quale il titolare del trattamento "*risponde per il danno cagionato dal suo trattamento che violi il presente regolamento*", mentre il responsabile del trattamento "*risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento*". Inoltre al fine di garantire il risarcimento effettivo dell'interessato è prevista una responsabilità di tipo solidale ogni qualvolta siano responsabili entrambi i soggetti del danno causato, così come stabilito dal paragrafo 4. È prevista inoltre la possibilità per il titolare o il responsabile che abbia ripagato per intero il risarcimento del danno, il diritto per tale soggetto di reclamare dagli altri titolari e/o responsabili l'ammontare di quota corrispondente la loro parte di responsabilità, come riportato dal paragrafo 5.

risarcimento del danno a favore dell'interessato che abbia subito il danno. Al paragrafo 3 dello stesso articolo 82 è prevista una clausola d'esonero della responsabilità per il titolare e il responsabile del trattamento, nella parte in cui prevede che "*il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile*". Dunque la conformità alle regole e i dettami del Regolamento da parte del titolare e del responsabile del trattamento permette di evitare, da un lato, il rigoroso regime di responsabilità, che come visto prevede una complicata prova di *compliance* al fine di dimostrare l'adeguatezza dell'azione intrapresa, dall'altro lato, le severe sanzioni previste dall'ultima parte del Capo VIII.

2.9.1 Apparato sanzionatorio

Per quanto riguarda l'apparato sanzionatorio non ci sono state rilevanti novità rispetto alla Direttiva 95/46/CE nel suo articolo 24, ma sicuramente il Regolamento, decidendo ancora una volta di valorizzare la pericolosità dell'attività di trattamento e l'importanza in termini di gravità di lesioni a cui possono essere sottoposti i dati personali degli individui, ha optato per un deciso inasprimento del regime sanzionatorio, elencando puntualmente modalità, condizioni e importi di erogazione[93]. Le disposizioni principali in tema sono individuate negli articoli 83 e 84, i quali disciplinano rispettivamente le

[93] A differenza della Direttiva 95/46/CE che si limitava all'articolo 24 intitolato "sanzioni" a prevedere che "*gli Stati membri adottano le misure appropriate per garantire la piena applicazione delle disposizioni della presente direttiva e in particolare stabiliscono le sanzioni da applicare in caso di violazione delle disposizioni di attuazione della presente direttiva*". Si ricorda in ogni caso che la direttiva del 1995 aveva lo scopo di armonizzazione della disciplina all'interno degli ordinamenti dei diversi Stati membri attraverso il recepimento di un nucleo condiviso di principi, valori e livelli minimi di tutela. Il Regolamento del 2016, invece, per sua natura (generale, vincolante, direttamente efficace e applicabile), richiede maggiore dettaglio e completezza.

"condizioni generali per infliggere sanzioni amministrative pecuniarie" e le altre "sanzioni".

In base all'articolo 83 è l'autorità di controllo competente ad infliggere e a determinare l'ammontare della sanzione amministrativa pecuniaria, purché quest'ultima sia in ogni singolo caso effettiva, proporzionata e dissuasiva. Colpisce infatti l'ampio margine di discrezionalità che il legislatore europeo affida all'autorità di controllo nella valutazione dell'*an* e del *quantum* della sanzione, valutazione che in ogni caso dovrà tenere in considerazione, volta per volta, alcuni elementi come:

- "*la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;*
- *il carattere doloso o colposo della violazione;*
- *le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;*
- *il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;*
- *eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;*
- *il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;*
- *le categorie di dati personali interessate dalla violazione;*
- *la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;*
- *qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del*

responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

- *l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e*
- *eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate direttamente o indirettamente, quale conseguenza della violazione*".

È specificato, inoltre, che tali sanzioni amministrative pecuniarie sono inflitte in aggiunta alle misure di cui all'articolo 58 paragrafo 2.

Secondo quanto previsto dai paragrafi 4, 5 e 6 dell'articolo 83, sono individuate tre tipologie di violazioni alle quali seguono tre sanzioni amministrative pecuniarie: identiche nelle modalità di erogazione, diverse per quanto riguarda l'ammontare della cifra, in modo tale che, a seconda dell'entità della violazione di specie, la sanzione possa assumere quei caratteri di proporzionalità, effettività e dissuasione sanciti nel paragrafo 1. Nel caso in cui siano violate le disposizioni riguardanti gli obblighi del titolare a norma degli articoli 8, 11, da 25 a 39, 42 e 43; oppure gli obblighi dell'organismo di certificazione (articoli 42 e 43) o dell'organismo di controllo (articolo 41 paragrafo 4), l'autorità di controllo può comminare una sanzione amministrativa pecuniaria, "meno grave", fino a 10.000.00 di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. Le sanzioni "più gravi" sono previste, invece, qualora siano violate le disposizioni inerenti i principi di base del trattamento, le condizioni del consenso e i diritti degli interessati; i trasferimenti di dati personali verso paesi terzi o verso un'organizzazione internazionale; qualsiasi obbligo imposto da uno stato membro a norma del Capo IX del Regolamento ("disposizioni relative a specifiche situazioni di trattamento"); oppure a causa dell'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione del flusso di dati dell'autorità di controllo sulla base dell'articolo 58 paragrafo 2. Per queste

violazioni sono prevista sanzioni pecuniarie più severe che possono raggiungere un ammontare pari a 20.000.000 di euro e fino al 4% del fatturato mondiale annuo precedente, se superiore, per le imprese.

Il paragrafo 8 dell'articolo 83 stabilisce che, in ogni caso, il potere conferito alle autorità di controllo, nell'ambito dell'applicazione delle sanzioni pecuniarie, deve essere soggetto a garanzie procedurali adeguate e conformi al diritto dell'Unione e degli Stati membri, prevedendo un ricorso giurisdizionale effettivo e la garanzia dell'osservanza dei principi del giusto processo.

Infine, il legislatore europeo nell'articolo 84 decide di lasciare un margine di discrezionalità agli Stati membri, permettendo a questi ultimi di individuare le altre e ulteriori sanzioni per le violazioni del Regolamento. Un margine di operatività che soffre come unico limite quanto già previsto per le violazioni sanzionate dall'articolo 83, mentre per le altre violazioni il Regolamento richiede soltanto che siano adottati tutti i provvedimenti necessari per assicurare l'applicazione delle sanzioni e che queste ultime siano effettive, proporzionate e dissuasive.

Ancora una volta si nota il cambio di prospettiva della disciplina in tema di protezione dei dati personali rispetto alla Direttiva 95/46/CE, più orientata, di volta in volta, a tutelare il singolo nei confronti del titolare del trattamento. Il Regolamento invece mira a sanzionare severamente i trattamenti illeciti, in un'ottica ben più ampia rispetto la dimensione del singolo, protesa ad una protezione globale dei soggetti dai trattamenti illeciti, specialmente nel momento in cui il numero rilevante di dati trattati o la tipologia particolare del procedimento integrino rischi collettivi di rilevante dimensione o portata.

Importante in materia di sanzioni è fare riferimento ancora una volta alla nuova normativa italiana di raccordo, rappresentata dal D.Lgs. 101/2018. Il presente decreto ha introdotto nuove sanzioni idonee e conformi alle disposizioni dettate dal Regolamento europeo 679/2016.

2.10 Capi IX, X e XI

È opportuno fare, a questo punto, e per completezza, una menzione generale degli ultimi tre Capi contenuti nel Regolamento 2016/679.

Il Capo IX del Regolamento tratta le "disposizioni relative a specifiche situazioni di trattamento", e tale dicitura vuole sottolineare il fatto che sono previsti regimi diversi quando il trattamento dei dati riguarda particolari categorie di soggetti o di attività professionali. Già nella prima disposizione del Capo presente, l'articolo 85 (Trattamento e libertà d'espressione e di informazione), sono previste varie esenzioni rispetto alla disciplina sancita dal Regolamento nel caso in cui vi siano scopi giornalistici o accademici riguardanti il trattamento dei dati, in modo da conciliare la protezione dei dati col diritto alla libertà d'espressione e di informazione. L'articolo 88 invece parla del "trattamento dei dati nell'ambito dei rapporti di lavoro", e stabilisce che possono essere previste norme più specifiche per assicurare la protezione dei dati dei dipendenti , in particolare per finalità di assunzione o esecuzione del contratto di lavoro, nonché quella del rispetto delle garanzie previste dalla contrattazione collettiva.

Gli ultimi due articoli del Capo IX del Regolamento, 90[94] e 91[95], non si discostano da quelli già analizzati, poiché prevedono, rispettivamente, deroghe quando si è di fronte ad autorità o soggetti dotati di segreto professionale od obbligo di segretezza, e la possibilità di applicare corpus religiosi nel caso di loro concordanza col Regolamento stesso.

Il Capo X del GDPR contiene solamente due articoli, il 92 e il 93, che riguardano rispettivamente il potere di adottare atti delegati conferito alla Commissione e il fatto che la stessa Commissione sia assistita da un comitato.

L'ultimo Capo, il numero XI, contiene le "disposizioni finali":

- abrogazione della Direttiva 95/46/CE a decorrere dal 25 maggio 2018 (art. 94);

[94] "Obblighi di segretezza".
[95] "Norme di protezione dei dati vigenti presso chiese e associazioni religiose".

- rapporto con la Direttiva 2002/58/CE, il quale rimane in vigore per quanto riguarda il trattamento nel settore della fornitura di servizi di comunicazione elettronica (art. 95);
- rapporto con accordi precedentemente conclusi (entro il 24 maggio 2016), i quali rimangono in vigore fino ad una loro futura modifica (art. 96);
- relazioni della Commissione (art. 97);
- riesame di altri atti legislativi dell'Unione in materia di protezione dei dati (art. 98);
- entrata in vigore e applicazione a decorrere dal 25 maggio 2018 (art. 99).

CAPITOLO 3

EVOLUZIONE DELLA NORMATIVA ITALIANA:

DIFFERENZE TRA CODICE DELLA PRIVACY E GDPR

Evoluzione della normativa italiana: differenze tra codice della privacy e GDPR

Il nuovo Regolamento europeo sulla protezione dei dati personali ha, come analizzato in precedenza, apportato numerose novità nel panorama dell'Unione. Trattandosi di un Regolamento Europeo, il quale per definizione è direttamente applicabile in tutti i suoi elementi, ha comportato per l'Italia l'obbligo, come per tutti gli altri Stati membri, di adeguarsi alla nuova disciplina.

È doveroso richiamare quanto già accennato nel primo capitolo, ovvero che la normativa vigente in Italia al momento dell'emanazione del Regolamento 679/2016 era ed è tutt'ora il Codice della Privacy, rappresentato dal D.Lgs. 196/2003. Il Codice era il risultato del recepimento delle Direttive 95/46/CE e 2002/58/CE e rappresentava, nonostante la sua lunghezza e presenza di allegati, una summa generale in materia di *privacy*. Con l'entrata in vigore del nuovo Regolamento in data 25 maggio 2018, vi è stata solo l'abrogazione della Direttiva 95/46/CE ma non quella del Codice della Privacy, il quale resta in vigore ed è perfettamente applicabile fin quando compatibile con il GDPR; in caso di incompatibilità su determinate situazioni, naturalmente verrà applicato il Regolamento e non il Codice.

Per favorire l'adattamento del GDPR in Italia, però, è da poco entrato in vigore il D.Lgs. 101/2018, precisamente il 19 settembre del 2018. Tale Decreto ha come scopo quello di abrogare le disposizioni del D.Lgs 196/2003 non più compatibili con il GDPR introducendone nuove, ma anche integrare e modificare le disposizioni che rimangono in vita, favorendo l'adattamento della disciplina italiana a quella europea. Il prodotto finale è una versione del codice più ridotta ma anche più coerente con la normativa comunitaria. Tale decreto è stato emanato nel rispetto di quanto sancito dall'articolo 13[96] della legge 163/2017 che contiene

[96] L'articolo 13 della legge 163/2017 porta la rubrica "Delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 679/2016 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al

una delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del Regolamento 679/2016. La tecnica legislativa adottata dal legislatore è stata quella di evitare di duplicare alcune disposizioni, molto simili ma non coincidenti, presenti sia nel Regolamento che nel Codice, operando così una scelta chiara.

Il decreto 101/2018, quindi, evita l'abrogazione del Codice della Privacy, che resta la normativa di riferimento nel panorama italiano in tema di *privacy*, il quale, però, si adatta decisamente alla disciplina comunitaria.

Nonostante la convivenza di entrambe le disposizioni sopracitate (Codice della Privacy e GDPR), esse presentano tra loro notevoli differenze che saranno oggetto di attenta disamina nel prosieguo della presente trattazione.

3.1 Armonizzazione della disciplina sulla protezione dei dati.

Un primo aspetto importante nonché risolutivo di differenza rispetto al passato consiste nel fatto che il Regolamento 679/2016 ha ultimato l'opera di uniformazione in due dimensioni, quella della disciplina in materia di *privacy*, e l'altra che consiste nella uniformazione delle varie discipline statuali in un'unica disciplina armonica valevole per ogni Stato membro dell'Unione Europea. Questa armonizzazione della disciplina ha come obiettivo finale quello di impedire eventuali disparità di trattamento per i soggetti interessati del trattamento che in passato potevano essere causate dall'applicazione di una disciplina di uno Stato anziché quella di un altro.

---

trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE". Inoltre recita al comma 1: "*Il Governo è delegato ad adottare, entro sei mesi dalla data di entrata in vigore della presente legge, con le procedure di cui all'articolo 31 della legge 24 dicembre 2012, n. 234, acquisiti i pareri delle competenti Commissioni parlamentari e del Garante per la protezione dei dati personali, uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*" […].

Nel testo del Regolamento 679/2016 vi è riferimento al concetto appena espresso nei Considerando numeri 103[97] e 167[98].

3.2 Concetto di *privacy*.

Un aspetto di profonda novità rispetto al passato riguarda il concetto di *privacy*. Nel Codice la Privacy era intesa come elemento finale delle attività di trattamento, in quanto eventuali vizi nella raccolta dei dati potevano essere sanati anche dopo che i trattamenti erano già stati effettuati. L'interessato vede garantito il proprio diritto di accesso a tutte le informazioni pertinenti alla sua persona detenute e trattate da terzi all'articolo 7[99], il quale ricomprende la possibilità di conoscere l'autore del trattamento, i fini dello stesso e i soggetti a cui tali dati possono essere ceduti; l'interessato, inoltre, ha la facoltà di verificare che i propri dati detenuti da terzi corrispondano al vero. In caso di lesione nei diritti sui propri dati si può ricorrere al Garante per la protezione dei dati personali o al giudice civile, ma solo una volta che il trattamento è stato ultimato, non a priori né durante lo stesso.

---

[97] "*La Commissione può decidere, con effetto nell'intera Unione, che un paese terzo, un territorio o un settore specifico all'interno di un paese terzo, o un'organizzazione internazionale offrono un livello adeguato di protezione dei dati, garantendo in tal modo la certezza del diritto e l'uniformità in tutta l'Unione nei confronti del paese terzo o dell'organizzazione internazionale che si ritiene offra tale livello di protezione. In tali casi, i trasferimenti di dati personali verso tale paese terzo od organizzazione internazionale possono avere luogo senza ulteriori autorizzazioni. La Commissione può inoltre decidere, dopo aver fornito una dichiarazione completa che illustra le motivazioni al paese terzo o all'organizzazione internazionale, di revocare una tale decisione*".

[98] "*Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, dovrebbero essere attribuite alla Commissione competenze di esecuzione ove previsto dal presente regolamento. Tali competenze dovrebbero essere esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio. A tal fine, la Commissione dovrebbe contemplare misure specifiche per le micro, piccole e medie imprese*".

[99] L'articolo 7 del Codice della Privacy è rubricato "diritto di accesso ai dati personali ed altri diritti" ed afferma al comma 1 che "*l'interessato ha il diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile*". Nei commi successivi sono previsti i diritti che appartengono all'interessato, sulla natura dei dati, sulla modificazione di essi e sulla possibilità di opposizione al trattamento.

Nel Regolamento 679/2016 cambia lo scenario previsto dal Codice della Privacy grazie all'introduzione di due principi di fondamentale importanza, definiti "*privacy by design*" e "*privacy by default*", previsti dall'articolo 25[100], che i titolari dovranno seguire e a cui dovranno sempre attenersi nell'applicazione pratica del trattamento. In particolare, con l'espressione "*privacy by design*", il Regolamento punta a richiamare l'attenzione dei titolari sull'esigenza che la protezione dei dati personali venga garantita fin dalla progettazione. A tal proposito, l'articolo 25 paragrafo 1[101] stabilisce che il titolare del trattamento dei dati personali deve adottare delle misure tecniche e organizzative idonee a dare concreta attuazione a quelle che sono le disposizioni e i principi in materia di protezione dei dati e garantire in questo modo i diritti degli interessati. Una delle particolarità di questa norma sta nel fatto che la predisposizione delle misure necessarie è prescritta sia nel momento in cui il titolare del trattamento deve determinare i mezzi del trattamento stesso, sia quando pone in essere le vere e proprie operazioni di trattamento. Il titolare non dovrà applicare misure standard e predeterminate, ma dovrà sempre procedere ad un'analisi realistica e specifica del singolo contesto di riferimento (approccio *risk-based* o basato sulla valutazione del rischio). Il secondo concetto introdotto dal GDPR, sempre all'articolo 25 ma nel suo paragrafo 2[102], è quello di "*privacy by default*". Con questa espressione il legislatore europeo ha affermato la necessità che la protezione dei dati personali

[100] "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita".
[101] "*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati*".
[102] "*Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica*".

sia garantita per impostazione predefinita: ne deriva che tutte le valutazioni che il titolare del trattamento deve effettuare in tema di protezione dei dati personali devono essere compiute a monte, cioè prima del trattamento, tenendo a mente i principi fondamentali di tutela della normativa, quali la liceità, la proporzionalità, la minimizzazione dei trattamenti nonché la trasparenza delle informative verso gli interessati. Seguendo tale criterio, il titolare deve svolgere un'analisi preventiva della situazione complessiva e adottare un approccio pratico che si dovrà, a sua volta, concretizzare in una seria di attività specifiche e dimostrabili. Le soluzioni a cui il titolare del trattamento potrà affidarsi potranno consistere, ad esempio, nella riduzione al minimo del trattamento dei dati personali, nella pseudonimizzazione dei dati personali, nella massima trasparenza sulle finalità e sulle modalità del trattamento di dati personali, nel consentire all'interessato di controllarne il trattamento rendendo facilmente ed effettivamente esercitabili i diritti previsti dal Regolamento. Il titolare dovrà attenersi a questi criteri in tutte le fasi del trattamento.

3.3 Individuazione della legge applicabile.

Spostandoci sul versante della disciplina da applicare di caso in caso, è immediatamente rinvenibile una differenza significativa tra Codice e Regolamento. Il Codice della Privacy per definire la legge applicabile considerava la sede del titolare del trattamento, a norma del suo articolo 5[103]. Il Regolamento, invece, ex articolo 3[104] ("ambito di applicazione territoriale") considera quale

[103] "Oggetto ed ambito di applicazione": 1."*Il presente codice disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato*" […]

[104] "1) *Il presente 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*. 2) *Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:* a)

legge applicabile quella del soggetto interessato del trattamento, ed i titolari (tra i quali anche social network, piattaforme web e motori di ricerca) saranno quindi soggetti alla normativa europea anche se aventi sede al di fuori dell'Unione. La norma di riferimento presenta quindi come prima novità il fatto che si riferisce, alternativamente, al titolare o al responsabile: è sufficiente infatti che lo stabilimento del responsabile del trattamento si trovi nel territorio dell'UE per far scattare le tutele previste dal Regolamento. La seconda ipotesi prevista dal legislatore comunitario poi scardina del tutto il tradizionale principio di stabilimento, così come previsto dal Codice della Privacy, sancendo che il Regolamento si applica al trattamento di dati personali di interessati che si trovano nell'Unione, indipendentemente da dove si trovi il titolare o il responsabile del trattamento. L'operatività della norma, però, è condizionata al fatto che le attività di trattamento riguardino l'offerta di beni o la prestazione di servizi agli interessati o il monitoraggio del loro comportamento all'interno dell'UE. La *ratio* alla base della scelta normativa si fonda sull'assunto che un soggetto sito nel territorio dell'Unione non può subire un trattamento dei propri dati personali meno tutelato, solo perché chi tratta dati risiede altrove. Ormai, nell'ambito del trattamento dei dati, la localizzazione geografica assume un rilievo sempre meno decisivo. Il Regolamento individua tassativamente le condizioni affinché sia possibile l'estensione territoriale del trattamento dei dati personali. Il considerando 23 del GDPR precisa, inoltre, che non basta l'accessibilità del sito web o l'indirizzo di posta elettronica o di altre coordinate di contatto o l'impiego di una lingua abitualmente utilizzata nel Paese terzo affinché si abbia l'offerta di beni o servizi. Si rientra nella previsione normativa quando il titolare o il responsabile usa una

l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; *oppure* b) *il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione*. 3) *Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico*".

lingua o una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni e servizi in tale altra lingua.

3.4 L'informativa.

Un aspetto da non trascurare, che propone alcune differenze con la precedente disciplina, è quello che riguarda le disposizioni recanti gli obblighi sull'informativa. L'informativa, così come disciplinata dall'articolo 13 del D.Lgs 196/2003, deve contenere tutti gli elementi necessari affinché l'interessato possa esercitare i propri diritti e manifestare un legittimo consenso. È obbligo di ogni titolare del trattamento definire per la propria organizzazione, un modello di gestione *privacy* che prenda in considerazione misure di sicurezza organizzative attraverso le quali si possa controllare la conformità legislativa dei modelli di informative elaborati. L'interessato, infatti, ha il diritto di essere informato in modo trasparente, leale e dinamico sui trattamenti effettuati sui suoi dati. Pertanto, affinché un trattamento possa definirsi trasparente, chiaro e corretto, è necessario che all'interessato sia resa un'informativa esaustiva sull'esistenza del trattamento e delle sue finalità. In particolare, l'informativa deve contenere:

- finalità: per quale scopo verranno trattati i propri dati personali;
- modalità di trattamento dei dati personali riferibile soprattutto alle misure di sicurezza adottate al fine di eseguire il trattamento nel rispetto dei principi di riservatezza, integrità e disponibilità dei dati;
- se il conferimento dei propri dati personali è obbligatorio o facoltativo;
- le conseguenze di un eventuale rifiuto a rendere disponibili i propri dati personali;
- a chi saranno comunicati o se saranno diffusi i propri dati personali;
- i diritti previsti dall'articolo 7 del Codice;

- chi è il titolare e, se è stato designato, il responsabile del trattamento[105].

Ciò che sicuramente cambia col nuovo Regolamento 679/2006 sono le nuove caratteristiche dell'informativa, la quale deve essere:

- concisa;
- trasparente;
- intellegibile;
- facilmente accessibile;
- con un linguaggio semplice e chiaro, in particolar modo se si tratti di minori.

Col GDPR l'informativa deve essere fornita in modo organico, redatta in un linguaggio semplice, senza frammentazioni e reiterazioni. Le informazioni essenziali devono essere offerte in un quadro di lealtà e correttezza nel rispetto della riservatezza dei dati. Se possibile, bisogna predisporre un'informativa breve, indicando con immediatezza le principali caratteristiche del trattamento. Secondo gli articoli 13 paragrafo 1 e 14 paragrafo 1 del Regolamento, l'informativa diventa più chiara e sintetica per facilitare la comprensione dei contenuti da parte di tutti gli interessati, grazie anche all'adozione di icone standardizzate, che saranno definite dalla Commissione Europea, identiche in tutta l'Unione Europea. I contenuti dell'informativa, dunque, risulteranno essere più ampi rispetto al Codice. In particolare, se i dati personali sono raccolti direttamente presso l'interessato, nella nuova informativa deve essere specificato:

- la base giuridica, ossia l'origine del trattamento (in una norma o contratto) specificando, inoltre, il suo interesse legittimo o da parte di terzi;
- se il titolare trasferisce i dati personali in Paesi terzi e attraverso quali strumenti;
- il periodo di conservazione dei dati;

[105] Elenco presente all'articolo 13 paragrafo 1 del Codice della Privacy, D.Lgs. 196/2003.

- il diritto dell'interessato di presentare un reclamo o un ricorso giurisdizionale all'Autorità di controllo;
- 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 (diritto all'oblio) oltre al diritto alla portabilità dei dati, altra novità introdotta dal Regolamento consistente nella possibilità di richiedere al titolare una copia dei dati oggetto del trattamento;
- se si effettua attività di profilazione automatizzata (*profiling* dei dati personali) e le possibili conseguenze che ne possano derivare;
- ulteriori informazioni utili per garantire maggiore trasparenza e correttezza all'interessato per il trattamento dei propri dati personali.

Naturalmente vi sono anche punti di contatto tra la disciplina del passato e quella del presente: se la raccolta dei dati viene fatta presso terzi, è possibile redigere una sola informativa, riferita sia ai dati conferiti direttamente dall'interessato sia ai dati acquisiti presso terzi. Secondo il Garante, sarebbe opportuno che le informative più articolate fossero basate su uno schema indicativamente più uniforme per il settore di attività. A tal proposito, ad esempio, le associazioni di categoria dovrebbero predisporre informazioni-tipo per determinati settori o categorie di trattamento. Il Garante precisa, inoltre, che deve invece essere fornita un'informativa specifica ad hoc, se il trattamento ha caratteristiche particolari quando, ad esempio, "coinvolge il trattamento di dati genetici, o può comportare rischi specifici per gli interessati".

Per quanto riguarda i tempi dell'informativa, la nuova disciplina stabilisce che nel caso di dati personali non raccolti direttamente presso l'interessato, l'informativa deve essere fornita entro un termine ragionevole che non può superare un mese dalla raccolta, oppure al momento della comunicazione (non della registrazione) dei dati se si tratta dei dati presi da terza parte. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore

trattamento, egli deve fornire all'interessato informazioni in merito alle diverse finalità. Se si dispone già dell'informazione necessaria, se la registrazione o la comunicazione dei dati personali sono già previste per legge o i dati in essere appartengono a dati di ricerca scientifica, storica o statistica, l'obbligo di presentazione di apposita normativa, in capo al titolare, può essere derogato. Infine sono previste sanzioni di natura amministrativa nei casi di omessa o inidonea informativa ai soggetti interessati.

3.5 Il consenso.

Dopo aver descritto la differenza tra normativa passata e presente riguardante l'informativa, viene naturale trattare il tema del consenso. Nel Codice della Privacy il consenso è trattato all'articolo 23, il quale recita:

1. *Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato.*
2. *Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.*
3. *Il consenso è validamente prestato solo se è espresso liberamente e specificatamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13.*
4. *Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili.*

Questa definizione risulta però in larga parte diversa da quella prevista dal GDPR, all'articolo 4[106] in combinato col Considerando 32[107].

Se il titolare decide di basare il trattamento sul consenso deve assicurarsi che esso presenti le seguenti caratteristiche:

- inequivocabile;
- libero;
- specifico;
- informato;
- verificabile;
- revocabile.

Per consenso inequivocabile si intende un consenso che può essere sia esplicito che implicito (non tacito), purché, nel momento in cui sia desunto dalle circostanze, non sussista alcun dubbio che col proprio comportamento l'interessato abbia voluto comunicare il proprio consenso (es. l'inerzia non può costituire manifestazione di consenso, come anche le caselle già spuntate). Vi deve essere una chiara azione positiva, inclusa anche l'azione di spuntare una casella od inserire la mail in un campo dove è specificata la finalità per la quale sarà usato il

[106] "*Il consenso dell'interessato è qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso esprime il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*".

[107] "*Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento di dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso*".

dato. Il consenso deve essere esplicito[108] nel caso di trattamento di dati sensibili o nel caso di processi decisionali automatizzati.

Il consenso poi deve essere dato liberamente, il che significa che l'interessato deve essere in grado di operare una scelta effettiva, senza subire intimidazioni o raggiri, né deve subire conseguenze negative a seguito del mancato conferimento del consenso[109].

Il consenso deve essere specifico, cioè relativo alla finalità per la quale è eseguito quel trattamento. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per ogni finalità.

Il consenso deve essere informato, occorre cioè che l'interessato sia posto in condizioni di conoscere quali dati sono trattati, con che modalità e finalità e i diritti che gli sono attribuiti dalla legge, cioè deve essere rispettato il principio di trasparenza. Inoltre l'interessato deve essere opportunamente informato sulle conseguenze del suo consenso (ad esempio deve essere indicato che in assenza di consenso non potrà accedere a determinate sezioni del sito web). L'informazione si ha attraverso l'apposita informativa, precedentemente descritta, che in questo caso diventa una vera e propria condizione di legittimità del trattamento. Il Regolamento europeo si concentra, più che sui requisiti formali del consenso, sulla necessità della validità sostanziale del consenso, per cui l'aspetto informativo è essenziale, richiedendo un linguaggio semplice e comprensibile, anche eventualmente colloquiale.

Per consenso verificabile, invece, non si intende un consenso che necessita una documentazione per iscritto, né che sia richiesta la forma scritta (anche se talvolta può essere preferibile, es. sui dati sensibili), ma che un'azienda, ad esempio, deve essere in grado di dimostrare che l'interessato lo ha conferito con riferimento a quello specifico trattamento. L'azienda in questione dovrà essere in

[108] Articolo 9 Regolamento 679/2006.
[109] Articolo 7 Regolamento 679/2006: "*Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto*".

grado di sapere anche a quale informativa l'utente ha acconsentito, distinguendo tra le varie versioni.

Il consenso infine può essere revocabile in qualsiasi momento. Così come per il consenso, la revoca non presenta forme particolari. Non vi è alcun obbligo di motivare la revoca, a seguito della quale il trattamento deve interrompersi, a meno che non sussista una differente base giuridica per continuare il trattamento; ovviamente la revoca non comporta l'illiceità del trattamento precedente, ma solo l'obbligo di terminare il trattamento. Per revocare il consenso, quindi, il titolare dovrebbe predisporre una procedura analoga a quella offerta per concedere il consenso. In alternativa è possibile revocare il consenso inviando una comunicazione, o tramite un apposito "*form*" sul sito, o tramite mail, ai contatti indicati nel sito all'interno dell'informativa (interpello al titolare). Nel caso in cui il titolare non ottemperi, ci si può rivolgere al Garante o al tribunale per la tutela dei propri diritti. Con la revoca si innesca il diritto di cancellazione.

Occorre tenere presente che il consenso non dura per sempre; quando si raccolgono dati personali occorre informare l'interessato della durata della conservazione, e quindi del trattamento del dato, scaduta la quale il dato va o anonimizzato oppure cancellato. Per tale motivo in alcuni casi potrebbe essere preferibile una base giuridica diversa dal consenso, come ad esempio i legittimi interessi del titolare del trattamento.

3.6 Trattamento dei dati: le figure.

Sono sicuramente interessanti da analizzare, in quanto elementi di evoluzione della normativa, quelli che riguardano propriamente il trattamento dei dati, sia sul versante delle figure implicate, sia sul controllo e tenuta dei dati sulle attività del trattamento stesso. Nel Codice della Privacy sono previste tre figure inerenti al trattamento dei dati, cioè il titolare del trattamento (articolo 28), il

responsabile del trattamento (articolo 29) e l'incaricato del trattamento (articolo 30). Le definizioni di tali figure sono presenti nell'articolo 4 del medesimo Codice:

- Per "titolare" si intende "*la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza*";
- "responsabile", invece, 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*";
- gli "incaricati" sono "*le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile*".

Una prima differenza tra Codice della Privacy e GDPR è sicuramente rappresentata dall'articolo 26 del Regolamento[110], che regola la situazione di contitolarità nel trattamento dei dati personali. Si tratta di una condizione che si verifica quando due o più titolari determinano congiuntamente le finalità e i mezzi del trattamento. Il Regolamento obbliga i contitolari a regolare il loro rapporto attraverso un contratto interno in cui, in maniera chiara, è necessario disciplinare:

- le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal regolamento;
- i rispettivi obblighi in merito all'esercizio dei diritti dell'interessato;
- le rispettive funzioni relativamente alla comunicazione dell'informativa, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti;
- indicare un punto di contatto utile agli interessati.

[110] "Contitolari del trattamento".

Sui medesimi contitolari gravano le medesime responsabilità relativamente agli obblighi derivanti dalle nuove norme e dunque entrambi sono passibili delle sanzioni previste per i titolari del trattamento. Nella situazione di contitolarità, l'interessato può esercitare i propri diritti, ai sensi del Regolamento, nei confronti di e contro ciascun titolare del trattamento; nella sostanza, ciò significa che, anche se tra i contitolari si è deciso che sia uno dei due ad occuparsi di trattare eventuali reclami o richieste di esercizio dei diritti, l'interessato potrà decidere diversamente, rivolgendosi all'altro titolare, avendo il diritto, come concessogli dal Regolamento, di ricorrere indistintamente ad uno dei due soggetti. Da un punto di vista delle informative e delle *privacy policy* pare possa ritenersi sufficiente che esse siano redatte in maniera congiunta, ma abbastanza chiara nel precisare la contitolarità del trattamento; non essendovi disposizioni sul punto, si può pensare, infatti, che il legislatore europeo abbia preferito lasciare agli attori liberi di gestire autonomamente questa parte di obblighi.

La differenza principale, però, riguarda le figure degli incaricati e dei responsabili interni, poiché non (espressamente) previste dal GDPR. Ciononostante, il Garante italiano considera non incompatibili con il Regolamento queste figure. Infatti, in un documento redatto dal Garante stesso, viene affermato che: "*Pur non prevedendo espressamente la figura dell'incaricato del trattamento, il regolamento non ne esclude la presenza in quanto fa riferimento a persone autorizzate al trattamento dei dati personali sotto l'autorità del titolare o del responsabile (articolo 4 n.10 Regolamento 679/2016)*". Quindi anche se il GDPR non prevede la figura autonoma dell'incaricato né del responsabile interno, questo non vieta che se il titolare o il responsabile del trattamento, oltre a fare tutto quello che il Regolamento espressamente prevede per "*le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile*"[111], vogliono anche fare, su base volontaria, una ulteriore responsabilizzazione di queste persone attraverso una specifica lettera di

[111] Articolo 4, "Definizioni", paragrafo 1, n.10, Regolamento 679/2016.

attribuzione di incarico e identificare queste persona utilizzando il termine "incaricato" o "responsabile interno", possono farlo.

Questa modalità operativa potrebbe anche essere considerata una buona prassi volta a poter ulteriormente sostenere la dimostrabilità della conformità al GDPR. Ma questa facoltà non deve essere intesa come un obbligo normativo come lo è invece per il Codice della Privacy la nomina a incaricato prevista dall'articolo 30, che al punto 2 prevede che la designazione dell'incaricato sia effettuata per iscritto e che nell'atto di nomina si debba individuare puntualmente l'ambito del trattamento consentito. Pur non essendo l'incaricato una figura giuridica autonoma del GDPR, il termine incaricato potrebbe essere comunque utilizzato nell'informativa o tra le informazioni fornite agli interessati, ma non con l'accezione di figura giuridica autonoma come previsto attualmente dal medesimo articolo 30 del Codice della Privacy.

In materia va segnalato l'articolo 2-quaterdecies del Decreto 101/2018, in tema di attribuzioni e compiti a soggetti designati. Il titolare o il responsabile del trattamento può prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento dei dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il titolare o il responsabile individua le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.

3.6.1 Trattamento dei dati: la documentazione.

Passando all'aspetto riguardante la tenuta di documentazione comprovante il regolare espletamento dei trattamenti dei dati, nel Codice della Privacy praticamente non vi erano obblighi particolari, a differenza del GDPR, nel quale è obbligatorio documentare tutti i trattamenti effettuati poiché è sufficiente non avere i documenti per essere passibili delle sanzioni stabilite dal Regolamento.

In particolare, nel D.Lgs. 196/2003, vi era l'obbligo di adottare un documento programmatico sulla sicurezza (DPS), poi abrogato, per tutte le imprese, lavoratori autonomi, enti o associazioni che trattavano dati personali. L'abolizione dell'obbligo di redazione del DPS, nei casi consentiti dalla normativa aggiornata, non solleva tuttavia dall'attuazione di tutti gli altri adempimenti *privacy* previsti dalla legislazione. Anzi, ne esce rafforzato proprio l'obbligo di implementazione concreta a discapito di un orpello solo burocratico e formale. D'altra parte, specie per le medio-grandi aziende, un documento analogo al DPS è pressoché scontato per motivi organizzativi e gestionali; per le piccole aziende o microimprese potrebbe, invece, essere utile un documento simile seppur semplificato in caso di sopralluoghi da parte degli enti predisposti. I contenuti del documento erano:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle altre relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento dei dati personali;

- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

3.6.2 Il registro delle attività di trattamento.

Col GDPR è stato istituito il registro delle attività di trattamento, un documento ove non solo il titolare ma anche il responsabile del trattamento possono rendicontare tutte le attività in materia di protezione e circolazione dei dati personali che li riguardano. La *ratio* è quella di dimostrare la conformità del trattamento alle disposizioni del Regolamento. Andando nello specifico, l'articolo 30 del Regolamento stabilisce l'obbligo di tenuta dei registri dell'attività di trattamento e i casi di esclusione.

Innanzitutto è bene ricordare che i registri delle attività di trattamento sono due: quello tenuto dal titolare del trattamento e quello del responsabile del trattamento dei dati. Il paragrafo 1 dell'articolo 30 del Regolamento parla del registro tenuto dal titolare del trattamento: "*Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:*

- *il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;*
- *le finalità del trattamento;*
- *una descrizione delle categorie di interessati e delle categorie di dati personali;*

- *le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di Paesi terzi od organizzazioni internazionali;*
- *ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;*
- *ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;*
- *ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1*".

Il paragrafo 2 del medesimo articolo descrive il registro tenuto dal responsabile del trattamento: "*Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:*

- *il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;*
- *le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;*
- *ove applicabile, i trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale, compresa l'identificazione del Paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;*

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

I paragrafi 3, 4 e 5 recitano rispettivamente:

- "*I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.*
- *Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.*
- *Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10*".

3.7 Le notificazioni sul trattamento.

Una differenza che si può definire sostanziale rispetto al passato riguarda il tema delle notificazioni. Bisogna partire dall'analisi del testo dell'articolo 37 del D.Lgs. 196/2003, rubricato "notificazione del trattamento", il quale prevede l'obbligo per il titolare di notificare al Garante della Privacy il trattamento di dati personali cui intende procedere nei casi il cui trattamento riguardi:

- dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;
- dati idonei a rivelare lo stato di salute e la vita sessuale, trattati ai fini di procreazione assistita, prestazione di servizi sanitari per via telematica

relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;

- dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;
- dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;
- dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;
- dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.

Lo stesso articolo 37 attribuisce, inoltre, al Garante la possibilità di individuare altri trattamenti suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato.

Con il nuovo Regolamento non si dovranno più effettuare le notificazioni all'Autorità Garante, ma per il titolare e i suoi rappresentanti sarà necessario tenere i registri delle attività di trattamento, che ricalcano il DPS, poiché ove possibile bisognerà documentare la descrizione delle misure di sicurezza adottate.

Nel Regolamento non è fatta dunque menzione della necessità, per i titolari, di procedere a notificazione al Garante nazionale in caso di trattamenti inerenti ai cosiddetti dati particolari. Si può quindi affermare che la nuova e cogente normativa europea ha "mandato in pensione" le notifiche che per anni

hanno caratterizzato i trattamenti di dati personali. È legittimo quindi parlare di implicita abrogazione dell'articolo 37 del Codice della Privacy, che rappresenta il punto di maggior rottura rispetto al passato come precedentemente anticipato. Alle autorità di controllo nazionali sono, in ogni caso, demandate funzioni di sorveglianza, promozione, consulenza, gestione di reclami, incoraggiamento ed esame dei codici di condotta, indagine, ingiunzione, nonché altri poteri di natura accertativa e sanzionatoria.

Una piccola parentesi va fatta anche sull'articolo 9 del Regolamento, che si occupa di dettare regole specifiche per trattamenti riguardanti categorie particolari di dati personali. I dati particolari presi in considerazione dal citato articolo sono i dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici e biometrici, i dati intesi ad identificare in modo unico una persona fisica, i dati relativi alla salute, alla vita sessuale o, ancora, all'orientamento sessuale della persona. Per questi dati vige il principio del divieto del trattamento, Eccezioni a tale regola generale sono dettate dallo stesso articolo 9, al paragrafo 2, in base al quale il divieto di trattamento non si applica al verificarsi di determinate condizioni.

Questa particolare categoria di dati personali è presa in considerazione anche dall'articolo 2-sexies del nuovo Decreto Legislativo 101/2018. Tale articolo pone l'accento sul trattamento di categorie particolari di dati personali, di cui all'articolo 9[112] del GDPR, necessario per motivi di interesse pubblico rilevante ed elenca una serie di materie in cui l'interesse pubblico si considera rilevante[113].

[112] "Trattamento di categorie particolari di dati personali".
[113] Ad esempio: accesso a documenti amministrativi e accesso civico; cittadinanza, immigrazione, asilo; controlli e ispezioni; obiezione di coscienza; gestione di rapporti di lavoro.

3.7.1 Le notificazioni sulle violazioni dei dati.

Rispetto alla materia delle notificazioni su alcune attività di trattamento, le quali erano necessarie nel Codice della Privacy e non previste nel GDPR, riguardo alle notificazioni sulle eventuali violazioni dei dati personali non era stabilito alcun obbligo nel Codice mentre è stato introdotto l'obbligo nel Regolamento 679/2016.

La disposizione in materia nel Codice della Privacy è rappresentata dall'articolo 167, "trattamento illecito di dati":

- "*Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.*
- *Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni*".

Il paragone con il Regolamento 679/2016 non può che partire dall'articolo 4 dello stesso Regolamento, che tra le varie definizioni che contiene contempla anche quella di "violazione dei dati personali"[114], la quale è considerata 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*"[115].

[114] "*Data Breach*".
[115] Articolo 4, "Definizioni", paragrafo 1, numero 12, Regolamento 679/2016.

Quindi, un *data breach* non è solo un evento doloso come un attacco informatico, ma può essere anche un evento accidentale come un accesso abusivo, un incidente, la semplice perdita di una chiavetta USB o la sottrazione di documenti con dati personali. Il nuovo Regolamento prevede specifici adempimenti nel caso di una violazione di dati personali. In caso di violazione dei dati il responsabile del trattamento, se designato, deve avvertire il titolare dell'avvenuta violazione dei dati. Quest'ultimo titolare dovrà, a quel punto, notificare l'evento all'autorità di controllo.

L'articolo 33 del GDPR prevede l'obbligo di notificare alle autorità di controllo la violazione dei dati, tranne il caso in cui "*sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persona fisiche*". La notifica deve avvenire "*senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza il titolare*". Qualora la notifica non avvenga nelle 72 ore, il titolare dovrà indicare i motivi del ritardo. La norma prevede anche la possibilità di allegare ulteriori informazioni in un momento successivo, per cui è preferibile comunque effettuare la notifica nelle 72 ore, anche se incompleta. Contrattualmente titolare e responsabile possono pattuire che la notifica alle autorità spetti al responsabile, sempre per conto del titolare. La notifica deve avere il contenuto previsto dall'articolo 33 del GDPR:

- descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie ed il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

La comunicazione della violazione dei dati agli interessati non è sempre prevista, poiché potrebbe creare un allarme generalizzato e portare ad un danno reputazionale significativo. Per questo si prevede l'obbligo di comunicare la violazione solo se è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persona fisiche. Il titolare del trattamento deve comunicare la violazione dei dati all'interessato senza ingiustificato ritardo, cosi come stabilito dall'articolo 34. Quest'ultimo prevede espressamente i casi nei quali non è richiesta tale comunicazione:

- il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati, di cui al paragrafo 1;
- la comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Per valutare i fattori che determinano il rischio per la libertà e i diritti degli interessati, sono stati successivamente fissati parametri determinati:

- tipo di *breach*: il tipo di violazione è un parametro per la valutazione del rischio. La violazione dei dati sanitari di tutti i pazienti di un ospedale è ben diversa dalla perdita dei dati sanitari di un singolo paziente;
- natura, numero e grado di sensibilità dei dati personali violati: l'accesso al nome e all'indirizzo dei genitori di un figlio rappresenta un rischio diverso rispetto all'accesso da parte dei genitori naturali del nome e dell'indirizzo dei genitori adottivi;

- facilità di associare i dati violati ad una persona fisica: può accadere che i dati violati non siano facilmente riconducibili ad una determinata persona fisica;
- gravità delle conseguenze per gli interessati: quando il titolare del trattamento percepisce il rischio che i dati oggetto della violazione possono essere utilizzati immediatamente contro gli interessati (es. sostituzione di persona);
- numero di interessati esposti al rischio: un parametro è sicuramente quello del numero degli interessati potenzialmente coinvolti;
- caratteristiche del titolare del trattamento: un attacco ad una struttura ospedaliera è certamente diverso dall'attacco ad una piccola azienda.

Comunque, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta, con ciò imponendo la comunicazione agli interessati.

Il titolare deve documentare le violazioni dei dati personali subite, tramite un apposito registro delle violazioni. Il registro dovrà contenere:

- data e ora della violazione;
- sorgente dell'informazione sulla violazione;
- conseguenze della violazione;
- data o ora della notifica della violazione all'autorità di controllo;
- motivo per il quale è stata ritardata o non è stata comunicata all'autorità di controllo;
- cause della violazione;
- provvedimenti adottati a seguito della violazione.

Tale documentazione dovrà essere fornita al Garante in caso di accertamenti.

In caso di mancato rispetto delle procedure di notifica della violazione si applica la sanzione amministrativa fino ad un importo di 10 milioni di euro oppure il 2% del fatturato dell'intera società. In caso di mancata notifica si configura anche l'assenza di adeguate misure di sicurezza, per cui si cumulano due distinte sanzioni.

3.8 I diritti dell'interessato.

Un'analisi molto approfondita va fatta in merito ai diritti dell'interessato: nel Codice della Privacy venivano riconosciuti al soggetto interessato diversi diritti, sebbene molti fossero di origine giurisprudenziale e di conseguenza non tassativamente tipizzati nel testo. Nel GDPR vengono codificati i diritti di elaborazione giurisprudenziale ai quali vengono affiancati diritti di nuova creazione come il diritto all'oblio e il diritto alla portabilità dei dati.

Partendo dal Codice, il titolo II della parte I regola i diritti dell'interessato[116]. In base all'articolo 7[117], comma 1, l'interessato ha, innanzitutto, "*diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile*". Nel comma seguente viene stabilito che l'interessato ha inoltre il diritto di ottenere l'indicazione:

- dell'origine dei dati personali che lo riguardano;
- delle finalità e modalità di trattamento;
- della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
- degli estremi identificativi del titolare, dei responsabili e del rappresentante designato;

[116] "Disposizioni generali". Gli articoli che trattano l'argomento sono gli artt. 7-10.
[117] "Diritto di accesso ai dati personali ed altri diritti".

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

L'interessato ha altresì diritto di ottenere:

- l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
- la cancellazione, la trasformazione in forma anonima o il blocco dei dati personali trattati in violazione della legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- l'attestazione che le operazioni di cui ai precedenti punti sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

L'interessato ha, infine, diritto di opporsi, in tutto o in parte:

- per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
- al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

I successivi articoli del Codice regolano poi l'esercizio dei diritti riconosciuti dall'articolo 7. Secondo quanto previsto dall'articolo 8[118], dunque, i diritti di cui sopra sono esercitati con "*richiesta rivolta senza formalità al titolare*

[118] "Esercizio dei diritti".

o al responsabile del trattamento", anche per il tramite di un incaricato, al quale è fornito idoneo riscontro senza ritardo. D'altra parte, i diritti di cui all'articolo 7 non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso al Garante per la protezione dei dati personali ai sensi dell'articolo 145[119] del Codice, se i trattamenti di dati personali sono effettuati nei casi elencati dal secondo comma dell'articolo 8. L'esercizio dei diritti, quando non riguarda dati di carattere oggettivo, può avere luogo salvo il caso in cui dovesse concernere la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o altri apprezzamenti di tipo soggettivo, nonché l'indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento.

L'articolo 9[120] del Codice prevede che la richiesta rivolta al titolare o al responsabile, di cui si è appena detto, possa essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. Il Garante può d'altra parte individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche. Quando riguarda l'esercizio dei diritti di cui all'articolo 7, commi 1 e 2, sopra esaminati, la richiesta può essere formulata anche oralmente e in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile. Nell'esercizio dei diritti di cui all'articolo 7, l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia. L'identità dell'interessato deve essere verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento. Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti od ordinamenti. La richiesta di cui all'articolo 7, commi 1 e 2, già

[119] "Ricorsi": "1. *I diritti di cui all'articolo 7 possono essere fatti valere dinanzi all'autorità giudiziaria o con ricorso al Garante*. 2. *Il ricorso al Garante non può essere proposto se, per il medesimo oggetto e tra le stesse parti, è stata già adita l'autorità giudiziaria*. 3. *La presentazione del ricordo al Garante rende improponibile un'ulteriore domanda dinanzi all'autorità giudiziaria tra le stesse parti e per il medesimo oggetto*".
[120] "Modalità di esercizio".

citati in precedenza, deve essere formulata liberamente e senza costrizioni e può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni.

Al fine di garantire l'effettivo esercizio dei diritti di cui all'articolo 7, secondo l'articolo 10[121] dello stesso Codice, il titolare del trattamento è tenuto ad adottare idonee misure volte, in particolare:

- ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili;
- a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico.

I dati sono estratti a cura del responsabile o degli incaricati e possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica. Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato deve comprendere tutti i dati personali che riguardano l'interessato comunque trattati dal titolare.

Passando all'analisi della corrispettiva disciplina nel Regolamento 679/2016, si può subito notare che vi è un importante cambio di prospettiva soprattutto nei confronti del cittadino, identificato come soggetto interessato. Costui, infatti, da mero spettatore, che ha assistito, soprattutto in passato, all'uso ed anche a volte all'abuso più vario dei propri dati, perdendone il controllo una volta comunicati per il trattamento, assume sempre più il ruolo di parte attiva del

[121] "Riscontro all'interessato".

rapporto, vedendosi riconoscere nuovi e più pregnanti diritti. Il Capo III del GDPR è dedicato proprio ai diritti dell'interessato e si prefigge lo scopo di delineare rapporti, poteri, diritti spettanti al soggetto che autorizza il trattamento dei propri dati affinché la comunicazione degli stessi non si esaurisca al solo momento del consenso bensì perduri nel tempo al fine di garantire un'adeguata protezione.

Nel Regolamento vengono, come precedentemente anticipato, codificati diritti di origine giurisprudenziale, affiancati da altri di nuova creazione:

- Richiesta del consenso → Cammina di pari passo ad ogni singola attività. Fornire il consenso comporta l'obbligo per la controparte di informare gli utenti interessati comunicando chi utilizzerà i dati e in che modalità. La richiesta del consenso sottoposta all'utente deve contenere le informazioni circa chi sarà il titolare del trattamento, gli eventuali destinatari nonché le finalità dell'utilizzo dei dati nel momento in cui gli stessi dati saranno ottenuti. In aggiunta alle predette informazioni, il titolare del trattamento fornirà all'interessato informazioni circa i suoi diritti di intervenire sull'utilizzo nonché sul periodo di conservazione dei dati.
- Tutele sulla prestazione del consenso → La prestazione del consenso è il primo atto di partecipazione attiva dell'utente e rappresenta l'accettazione, non obbligatoria, al trasferimento dei dati. Il consenso deve essere espresso mediante un atto positivo inequivocabile, libero e specifico. Non è vincolante il mezzo, potendo comunicarlo in forma scritta, mediante mezzi elettronici o oralmente. Ai fini di una valutazione della libertà del consenso particolare attenzione dovrà essere posta ai dati personali che vengono richiesti ed alla correlazione rispetto alla prestazione. Può capitare, infatti, che la richiesta di consenso per l'esecuzione di un contratto sia condizionata dall'autorizzazione al trattamento di dati non necessari. In casi come questi viene pregiudicata proprio la libertà del consenso manifestato dal cittadino nonché la violazione del principio di minimizzazione dei dati ossia il criterio secondo cui i dati richiesti devono essere adeguati, pertinenti e limitati rispetto alla finalità per la quale sono richiesti. Ciò che è anche

importante sottolineare è che il consenso non si esaurisce nel momento in cui viene prestato, non è una compravendita con la quale si trasferisce ad altri un bene, bensì si autorizza semplicemente la società che raccoglie i dati al trattamento degli stessi. Occorre che già all'atto della prestazione del consenso, il cittadino sia debitamente informato delle garanzie che saranno adoperate per tutelare i dati nonché i diritti che ha di accedere, di intervenire per controllare il trattamento, o di rettificare o anche ritirare il consenso.

- Divieto di trattare alcune categorie di dati personali → I dati non sono tutti uguali e le informazioni che riguardano la persona non hanno tutte lo stesso peso e lo stesso valore. Ci sono dati strumentali alla richiesta di attivazione di determinati servizi o contratti per i quali all'utente sarà sottoposto un modulo per fornire il consenso, e dati che non hanno, per loro stessa natura, alcun ruolo nella stipula di nuovi contratti. Per il primo tipo di dati indicati, il controllo che potrà essere fatto sull'operato del titolare del trattamento, nel momento in cui viene richiesto il consenso, sarà di tipo funzionale ed orientato al rispetto del principio della minimizzazione dei dati raccolti. Accanto a queste informazioni, vi sono poi categorie di dati, relative alla persona, per le quali vige il divieto di trattamento, superabile solo nel caso in cui vi sia un consenso esplicito prestato per assolvere a diritti e/o obblighi specifici, per tutelare interessi vitali o anche, tra l'altro, nel caso in cui sia l'interessato a renderli di dominio pubblico. Questi dati, che godono di particolare tutela, sono quelli inerenti l'origine razziale o etnica, le opinioni pubbliche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici, biometrici, relativi alla salute o alla vita sessuale o all'orientamento sessuale. Per il trattamento di dati relativi a condanne penali occorre il controllo della pubblica autorità. Questa particolare categoria di dati personali è presa in considerazione anche dall'articolo 2-sexies del nuovo Decreto Legislativo 101/2018, come già esaminato in precedenza.

- Diritto di accesso → La persona interessata ha sempre il diritto di ottenere dal titolare del trattamento la conferma che vi sia in corso un trattamento dei propri dati e, in caso positivo, accedere alle informazioni inerenti lo specifico trattamento, ossia sapere per quali fini sono stati adoperati i dati, quali dati sono stati adoperati, a chi sono stati comunicati, il periodo di tempo entro cui i dati saranno conservati o una previsione della durata, la possibilità di esercitare i diritti di rettifica, cancellazione o di limitazione all'uso dei dati, o anche il rifiuto del trattamento, così come il diritto di proporre reclamo presso l'autorità di controllo. Il diritto d'accesso rappresenta, proprio per il potere che conferisce all'utente, una porta aperta sull'operato del titolare del trattamento riconoscendo il grande potere, ad ogni persona fisica, di controllare nel tempo le tracce lasciate dai propri dati e di intervenire, eventualmente, per cambiare le cose. In sintesi è come se venisse riconosciuto il potere di controllare le conseguenze del consenso prestato e di correggerlo o cancellarlo, come pure solo di monitorarlo ottenendo le informazioni richieste, ricordando che quei dati sono e restano dell'interessato.
- Dovere di fornire le informazioni richieste → Il dovere di fornire le informazioni richieste è strettamente collegato alla richiesta del cittadino formulata nell'esercizio del diritto di accesso e rappresenta il riscontro che il titolare del trattamento ha il dovere di fornire all'interessato senza alcun aggravio economico, salvo il caso in cui risultino manifestamente infondate o eccessive. Quanto alla tempistica, è stato fissato un termine massimo di un mese, prorogabile nei casi di complessità o di elevato numero di richieste. Se non dovesse rispettarla, vengono ad attivarsi ulteriori diritti di azione riconosciuti all'interessato.
- Possibilità di proporre reclamo/ricorso → La possibilità di proporre reclamo/ricorso è riconosciuta al cittadino nel caso in cui il titolare del trattamento non riesca a fornire le informazioni richieste dall'interessato. Infatti, decorso il tempo di un mese o più, in caso di proroga, il titolare del

trattamento dovrà comunque informare delle sue difficoltà a fornire tempestivo riscontro, nonché della possibilità per il cittadino di adire, con reclamo, l'autorità di controllo oppure, con ricorso, l'autorità giurisdizionale.

- Diritto di rettifica → Il diritto di rettifica potrà essere esercitato ogni qualvolta l'interessato riscontri l'utilizzo di dati personali inesatti. L'inesattezza dei dati posseduti dal titolare del trattamento è un'ipotesi che può verificarsi molto più frequentemente di quanto non si pensi e che può avere anche conseguenze rilevanti per il cittadino. Da qui la necessità di fornire gli utenti del diritto ad ottenere la rettifica dei dati, al fine di evitare che l'errore possa danneggiarli o, comunque, avere conseguenze negative[122]. Dall'errore scaturiscono una serie di segnalazioni e/o conseguenze a catena che sarebbe oltremodo iniquo far gravare sull'utente, per cui un simile diritto, a fronte di siffatte situazioni, non può che essere considerato pienamente appropriato. Ovviamente se viene riconosciuto il diritto di chiedere la rettifica, al fine di rendere efficace la richiesta, occorre che alla stessa il titolare del trattamento dia seguito senza ingiustificato ritardo. Qualora la richiesta avesse ad oggetto l'integrazione di dati incompleti, potrà essere fornita una dichiarazione integrativa.
- Revoca del consenso → La revoca del consenso non è sottoposta ad alcun vincolo o condizione né di carattere temporale né di natura strutturale. Così come viene garantita la possibilità di esprimere un consenso libero, il regolamento garantisce il diritto di revocare il consenso con la stessa libertà. Il diritto di revocare il consenso è, pertanto, esercitabile in qualsiasi momento. Ovviamente il trattamento dei dati avvenuto nell'arco di tempo coperto dal consenso espresso, resta lecito. Inoltre, occorre che non siano stabilite modalità di revoca del consenso più articolate, finalizzate a

[122] Di casi, al riguardo, ce ne sono tanti: si pensi alla registrazione di dati errati quanto alle proprie abitudini di vita, come ad esempio essere o meno identificato come fumatore nella prenotazione di una camera d'albergo o nella stipula di una polizza vita, o anche quanto ad errori circa una erronea segnalazione quale cattivo pagatore.

disincentivare la revoca, rispetto a quelle di prestazione dello stesso. Di tale diritto il cittadino deve avere notizia già nel momento stesso in cui presta il consenso.

- Diritto all'oblio → Il diritto alla cancellazione dei dati, cosiddetto diritto all'oblio, è probabilmente uno dei diritti espressi con maggiore forza dal GDPR e che è altro rispetto al già esaminato diritto a revocare il consenso. Anzi, la revoca del consenso rappresenta uno dei possibili presupposti per ottenere la cancellazione dei dati personali. È un diritto fondamentale alla cui richiesta il titolare del trattamento deve adempiere, senza ingiustificato ritardo, cancellando i dati. La finalità principale di questo diritto riconosciuto all'utente è stretta conseguenza dell'uso di tecnologie sempre più avanzate che potrebbero compromettere l'immagine dell'utente continuando, ad esempio, a diffondere dati in violazione del consenso, in quanto revocato, oppure perché il trattamento dei dati è avvenuto illecitamente. Dietro questo tipo di tutela, possono esservi, pertanto, ragioni molto delicate che inducono l'interessato a chiedere l'oblio dei dati, ma anche il fatto che i dati trasmessi non siano più necessari alle finalità a suo tempo indicate può rappresentare un valido motivo per ottenerne la cancellazione. È, dunque, un diritto molto esteso che può essere limitato solo nella misura in cui se ne giustifichi la necessità al cospetto di più alto valore[123].
- Diritto di limitazione del trattamento → Il diritto di limitazione del trattamento rappresenta una ulteriore forte garanzia a tutela del cittadino attivabile ogni qualvolta vi sia una situazione da verificare o un conflitto tra interessato e titolare del trattamento. Al fine di evitare che questo tempo di sospensione necessario per dirimere l'eventuale controversia possa, pur esso, rappresentare un ulteriore aggravio per il cittadino, si è ritenuto opportuno creare una sorta si sospensione per mezzo della quale si opera

[123] Ad esempio diritto di libertà, espressione, informazione, obbligo legale.

una limitazione temporale del trattamento in attesa di conoscere la sorte dei dati. L'interessato può chiedere al titolare del trattamento, ed ha il diritto di ottenerla, una limitazione di uso dei dati. La sua portata è più estesa rispetto al semplice blocco del trattamento potendo, la richiesta, essere motivata facendo riferimento ad una contestazione sull'esattezza dei dati, su un ipotizzato trattamento illecito o anche perché ci si è opposti al trattamento.

- Diritto alla portabilità dei dati → Il diritto alla portabilità dei dati è predisposto, funzionalmente, sul riconoscimento del cittadino di trasmettere i propri dati, forniti ad un titolare del trattamento, ad altro titolare. È un diritto assoluto, cui il primo soggetto che ha ricevuto i dati non può opporsi né tantomeno creare impedimenti. Anzi, nel caso in cui fosse tecnicamente fattibile, l'interessato potrà ottenere la trasmissione diretta dei dati dall'uno all'altro.
- Diritto di opporsi al trattamento dei dati personali → Tale ultimo diritto può essere esercitato dal cittadino in qualsiasi momento. Non vi sono motivi particolari che devono essere addotti alla base della richiesta, ricevuta la quale, al titolare del trattamento non resterà altro da fare che astenersi dal trattare ulteriormente i dati, a meno che non dimostri l'esistenza di motivi legittimi cogenti che prevalgono su quelli dell'interessato. Anche questo diritto dell'interessato deve essere comunicato in sede di richiesta iniziale del consenso, rappresentando il potere di modificare nel tempo l'autorizzazione concessa col consenso e, pertanto, dando immediatamente concretezza, all'utente, della possibilità non solo di rivedere il consenso ma anche di opporsi al trattamento dei dati per motivi semplicemente connessi alla sua situazione particolare.

Un cenno importante riguardante il tema dei diritti dell'interessato va fatto al nuovo Decreto Legislativo 101/2018. Di particolare interesse è l'articolo 2-undecies, rubricato "limitazione ai diritti dell'interessato", che elenca una serie di situazioni in cui l'esercizio dei diritti dell'interessato di cui

agli articoli da 15 a 22 del GDPR e il reclamo di cui all'articolo 77 del medesimo Regolamento subiscono delle limitazioni, in quanto possono comportare un pregiudizio effettivo e concreto agli interessi tutelati in base alle disposizioni in materia di riciclaggio, allo svolgimento di investigazioni difensive o all'esercizio di un diritto in sede giudiziaria, alla riservatezza dell'identità del dipendente che segnala, ai sensi della legge 179/2017, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio[124]. Sempre rilevante in materia è l'articolo 2-terdecies del D.Lgs. 101/2018, che disciplina l'esercizio dei diritti di cui agli articolo da 15 a 22 del GDPR, qualora l'interessato sia una persona deceduta; tali diritti possono essere esercitati da chi ha un interesse proprio o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari e meritevoli di protezione.

3.9 Figura di raccordo tra soggetti del trattamento e Autorità Garante.

L'ultima differenza che merita di essere inserita in questa analisi è quella che riguarda l'esistenza o meno di una figura di raccordo tra i soggetti del trattamento e l'Autorità Garante. Nel Codice della Privacy una simile figura di raccordo non era neanche lontanamente prevista, mentre nel GDPR è stata introdotta la figura del Data Protection Officer (DPO). La figura del DPO, analizzata accuratamente nel capitolo precedente, è una figura professionale obbligatoria per alcune categorie di soggetti titolari del trattamento, che funge da referente con il Garante e deve avere requisiti e competenze elevate. È d'obbligo chiarire che tale figura può essere sia un dipendente che un collaboratore con regolare contratto.

[124] È il cosiddetto fenomeno del "*whistleblowing*". Il "*whislteblower*" è, a titolo esemplificativo, lo "spione".

CONCLUSIONI

Conclusioni

Come analizzato in questo elaborato, la *privacy* è un concetto che storicamente ha sempre creato dubbi in merito al suo contenuto e alla sua ampiezza. Numerosi studi, la dottrina, nonché varie sentenze si sono espresse nel corso dei secoli sull'argomento, accompagnandolo nella sua costante evoluzione che lo ha portato a ciò che è oggi, soprattutto sotto il punto di vista della protezione dei dati personali, oramai in continua circolazione nella società odierna.

Le numerose evoluzioni di questo diritto hanno creato terreno fertile affinché si elaborasse una disciplina il più possibile unica, certa e trasparente. Questa necessità, in Europa, è stato l'impulso decisivo alla redazione di una disciplina uniforme, contenuta nel Regolamento 679/2016, meglio conosciuto come GDPR (General Data Protection Regulation), emanato nel 2016 ed entrato in vigore il 25 maggio del 2018.

A quasi un anno dall'entrata in vigore del presente Regolamento, si può cominciare a fare un bilancio in merito al suo contenuto e alla sua reale efficacia.

Dalle prime testimonianze raccolte nelle sedi di discussione di questo argomento, emerge che l'obiettivo della "compliance totale" è ancora lontano. Ma forse una totale compliance non è il reale obiettivo prefissato dalla stessa normativa.

È possibile che non tutte le aziende e i cittadini in generale abbiano preso in considerazione la necessità di adeguamento, nel rispetto della diversità dei settori e degli Stati. In Italia probabilmente scontiamo un ritardo dovuto anche all'attesa del decreto 101/2018, entrato in vigore lo scorso 19 settembre, con l'intento di adeguare il nostro Codice della Privacy, D.lgs. 196/2003, alla nuova regolamentazione comunitaria. Di questa innovazione e delle evoluzioni riscontrate tra i due testi adesso in vigore nel nostro Paese ci siamo già occupati nei precedenti capitoli.

Va sottolineato però che molte aziende virtuose hanno intrapreso un percorso di adeguamento effettivo, anche se probabilmente non lo hanno completato del tutto.

Tra i tanti dubbi interpretativi della nuova disciplina, non pienamente chiari sicuramente possiamo elencare: la necessità o meno della nomina di un Data *Protection Officer* (DPO), quali debbano essere le misure di sicurezza da applicare di volta in volta, come e quando effettuare delle valutazioni di impatto, e altri ancora. La maggior parte delle aziende a tal proposito si affida a consulenti esterni, i quali possono essere di estrazione legale o di estrazione tecnica.

Il confronto effettuato tra "vecchio" Codice della Privacy e nuovo Regolamento europeo porta sicuramente ad un risultato positivo poiché la normativa è molto approfondita e dettagliata, disciplinando, tra le sue numerose disposizioni, aspetti che in passato erano stati trascurati, chiarendo quindi analiticamente punti storicamente fondamentali.

In conclusione, dopo aver trattato e descritto in maniera analitica il contenuto del GDPR, è possibile estrapolare gli elementi che effettivamente costituiscono oggetto di novità:

- *Privacy by design* e *Privacy by default*
- Principio di *accountability*
- *Data Protection Officer* (DPO)
- Registro delle attività
- Valutazione d'impatto sulla protezione dei dati
- Codice di condotta e di certificazione
- Nuove disposizioni su informativa e consenso
- Portabilità dei dati
- Diritto all'oblio
- Tutela in caso di *data breach*

BIBLIOGRAFIA

Bibliografia

A. DE CUPIS, I diritti della personalità, Giuffrè Editore, Milano, 1982.

A. RAVÀ, *Istituzioni di diritto privato*, CEDAM, 1938.

ARISTOTELE, *La politica*, a cura di C. A. Viano, BUR Biblioteca Univ., 2002.

F. DE STEFANI, *Le regole della privacy. Guida pratica al nuovo GDPR*, Hoepli, 2018.

F. GAUDINO, *Il GDPR "italiano",* http://www.diritto24.ilsole24ore.com/art/avvocatoAffari/mercatiImpresa/2018-09-12/il-gdpr-italiano-095527.php, Il Sole 24 Ore, 2018

F. GRADOZZI, *Privacy in regola*, Independently published, 2018.

F. DI RESTA, Le recenti modifiche al Codice della Privacy: note critiche, https://www.altalex.com/documents/news/2012/07/20/le-recenti-modifiche-al-codice-della-privacy-note-critiche, Altalex, 2012.

F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli Editore, 2016.

F. S. LANE, *American privacy: the 400-year history of our most contested right*, Beacon Press, 2009.

G. BUTTI e A. PIAMONTE, *GDPR: nuova privacy. La conformità su misura*, Iter Edizioni, 2017.

G. D'ACQUISTO e M. NALDI, *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Giappichelli Editore, 2017.

G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, TrE-Press, 2015

G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli Editore, 2017.

G. PUGLIESE, *Il preteso diritto alla riservatezza e le indiscrezioni cinematografiche*, Zanichelli, Bologna, 1954.

G. RESTA e V. ZENO-ZENCOVICH, *La protezione transnazionale dei dati personali: dai "Safe Harbour Principles" al "Privacy Shield",* Roma Tre Press, 2016.

G. VIDAL, *La fine della libertà. Verso un nuovo totalitarismo?*, Fazi, 2004.

L. MIGLIETTI, Profili storico-comparativi del diritto alla privacy, http://www.diritticomparati.it/profili-storico-comparativi-del-diritto-alla-privacy/, Diritti Comparati, 2014.

M. IASELLI e S. GORLA, *Storia della privacy*, http://www.micheleiaselli.it/storiadellaprivacy.pdf, Edizione Lex Et Ars, 2015.

M. SOFFIENTINI, *Privacy, protezione e trattamento dei dati*, IPSOA, 2018.

R. PANNETTA, *Consenso o non consenso? Ecco cosa cambia con il GDPR*, https://www.corrierecomunicazioni.it/privacy/gdpr/consenso-o-non-consenso-ecco-cosa-cambia-con-il-gdpr/, CorCom (Corriere Comunicazioni), 2018

S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, CEDAM, 2006.

S. WARREN e L. BRANDEIS, *The Right to Privacy. The Implicit made Explicit*, Harvard Law Review, 1890.

T. M. COOLEY, *Treatise on the law of Torts or the Wrong Which Arise Independently of Contract*, Callaghan e Company, 1907.

U. PAGALLO, *La tutela della privacy negli Stati Uniti d'America e in Europa*, Giuffrè Editore, 2008.

V. CUFFARO e F. DI CIOMMO, *Trattamento dei dati personali e Regolamento UE n. 2016/679*, IPSOA, 2018.