UNIVERSITÀ DEGLI STUDI DI PAVIA

DIPARTIMENTI DI GIURISPRUDENZA, INGEGNERIA INDUSTRIALE E DELL'INFORMAZIONE, SCIENZE ECONOMICHE E AZIENDALI, SCIENZE POLITICHE E SOCIALI, STUDI UMANISTICI

CORSO DI LAUREA INTERDIPARTIMENTALE IN

COMUNICAZIONE DIGITALE

IL GDPR E LA DISCIPLINA DEI SOGGETTI DEL TRATTAMENTO ALLA PROVA DELL'EVOLUZIONE TECNOLOGICA

Relatore:

Chiar.mo Prof. Emanuele Tuccari

Correlatore:

Chiar.mo Prof. Flavio Antonio Ceravolo

Tesi di laurea di Mattia Bera matr. n. 509854

ANNO ACCADEMICO 2024/25

Un calcolatore meriterebbe di essere definito intelligente se potesse ingannare un essere umano facendogli credere di essere umano.
("A. Turing").

INDICE

Capitolo 1
I SOGGETTI DEL TRATTAMENTO DA IERI A OGGI

Per iniziare questo elaborato è doveroso fare un *excursus* storico: dalla prima volta in cui si è iniziato a parlare giuridicamente di protezione dei dati personali in Europa fino ad oggi, ma solo dopo aver spiegato quali sono i problemi che hanno fatto nascere l'idea di scrivere questa Tesi.

1.1 **Quesito di ricerca**

Il problema su cui verte questa Tesi magistrale è il futuro dei soggetti del trattamento nel GDPR in relazione a determinate tecnologie: *cloud computing*, *robot*, domotica, *smart cars* e intelligenze artificiali generative.

Ciò che ha stimolato la curiosità dell'autore e che ha portato alla stesura di questa Tesi è ricercabile nelle criticità che risiedono nella struttura dei soggetti del trattamento nel GDPR, che verranno spiegati nelle prossime pagine. Si potrà ravvisare come il rapporto tra le due figure del titolare e del responsabile del trattamento abbia mantenuto una natura di tipo verticistico, che, pur essendosi allargato in merito agli obblighi e alle misure di sicurezza, nella sua struttura risulta poco elastico ai cambiamenti risultanti dall'evoluzione tecnologica in atto. I due principali casi che hanno portato a farsi delle domande sono rappresentati da due pareri del Gruppo di lavoro art. 29; questi sono precedenti al GDPR, ma i dubbi sollevati sono rimasti intatti ancora adesso. *In primis*, si fa riferimento al parere del 1 luglio 2012 n. 5 con riguardo al *cloud computing*, con il quale si arrivò a concludere che siccome era il cliente a decidere in merito all'assegnazione in parte o nella totalità del trattamento ai servizi di *cloud*, allora sarebbe risultato lui come titolare del trattamento. Ciò, oltre a rappresentare una forzatura, crea vari problemi, specie con riferimento agli obblighi posti in capo al titolare del trattamento. Il secondo parere è il n. 8 del 16 settembre 2014, riguardo alle tecnologie *IoT* (*Intenet of things)*,

con cui si affermò che nel contesto di questi servizi, come per esempio i dispositivi domotici, gli utilizzatori risultino responsabili del trattamento mentre i fornitori e produttori dei *software* installati e in alcuni casi le terze parti abilitate a interagire con il dispositivo sono considerati i titolari del trattamento.

Il fatto che un soggetto interessato dal trattamento di dati personali possa ricoprire in un caso la figura del titolare e nell'altro quella del responsabile risulta problematico. La riflessione ha portato a domandarsi su quali tecnologie possano ripercuotersi questi problemi, poiché ormai il *cloud computing* in primis è utilizzato da un'ampia gamma di prodotti digitali e anche nei dispositivi *IoT*, aggiungendo a ciò il culmine dell'evoluzione delle tecnologie *IA* negli ultimi due anni. Tutto questo ha portato a chiedersi fin dove potessero espandersi queste due problematiche e se ce ne siano di nuove su cui riflettere, per cui dopo aver spiegato l'evoluzione giuridica della protezione dei dati personali si darà una definizione completa delle cinque tecnologie citate e del volume economico rappresentato, successivamente la riflessione passerà alle criticità giuridiche derivanti da queste tecnologie e alla loro esauriente esplicazione, in conclusione saranno proposte delle soluzioni e delle linee su cui probabilmente si andrà a parare, capendo anche il rapporto che ci potrà essere con il *Regolamento E-privacy* e *l'Artificial Intelligence Act*.

1.2 La Convenzione 108 del Consiglio d'Europa

L'origine del diritto alla protezione dei dati personali è moderna, dipendendo strettamente dal progresso tecnologico. Bisogna rivolgere lo sguardo in America nel periodo di fine Ottocento e di inizio Novecento, dove si iniziò a trattare il diritto alla privacy con il significato collettivo di "*diritto di essere lasciati soli*". I motivi di questa novità vanno ricercati in due tendenze di quel periodo: *in primis*, si devono considerare i mutamenti culturali derivanti dagli ideali individualistici e liberali della borghesia; in secondo luogo, il progresso tecnologico di fine Ottocento aveva portato novità immense come il telefono e la fotografia[1].

[1] Cfr. A.M. Garofalo, *Introduzione al diritto alla protezione dei dati e al GDPR* in G. Magri, S. Martinelli, S. Thobani (a cura di), *Manuale di diritto privato delle nuove tecnologie*, I ed., Torino, 2022, 93.

In Europa, nel secondo Dopoguerra, si può osservare come il diritto alla protezione dei dati personali non goda di nessuna tutela fondamentale, ma viene trattato come diritto singolo, mentre quelli alla riservatezza e alla vita privata vengono concepiti come diritti fondamentali[2]. Le ragioni vanno ricercate nel fatto che la tecnologia non veniva considerata così determinante per l'evoluzione del diritto, nonostante i trattamenti automatizzati di dati ebbero un largo utilizzo bellico e fecero capire la loro portata[3]. Persino la CEDU, firmata a Roma il 4 Novembre 1950, conteneva solamente all'art. 8 il diritto al rispetto della vita privata e familiare. L'elemento che si intende evidenziare è che fino a questo momento ancora non si era trattato di protezione dei dati personali[4].

Nel contesto storico della protezione dei dati personali, si sono delineati scenari in cui le posizioni consolidate nel dibattito dottrinale e giurisprudenziale sui rischi per la riservatezza delle informazioni hanno coinciso con l'ascesa di nuovi strumenti tecnologici. Questi strumenti non solo minacciavano la libertà individuale di autodeterminazione informativa, ma segnavano anche una svolta nell'ambito informatico. L'avvento dei computer, dotati di una capacità di gestione delle informazioni senza precedenti, impattava direttamente sull'*informational privacy*, portando a un cambiamento radicale rispetto alle intrusioni mediatiche del passato.

Mentre in passato giornali e programmi televisivi diffondevano spesso informazioni personali senza consenso, l'era digitale rivelava una nuova frontiera di invasione della privacy basata sulla raccolta e l'elaborazione dei dati personali. Questa trasformazione si manifestava con l'informatizzazione delle banche dati, inizialmente nel settore amministrativo e bancario, per poi estendersi anche alle imprese private. Tuttavia, l'accesso a tali tecnologie rimaneva limitato inizialmente a causa dei costi elevati, ma l'evoluzione tecnologica rendeva presto questi strumenti più accessibili. Con l'avvento dei computer domestici, si assisteva alla

[2] Cfr. F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo*, I ed., Torino, 2016, 56.
[3] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* cit., p. 57.
[4] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* cit., p. 58.

democratizzazione dell'informatica, trasformando questi strumenti in strumenti quotidiani per una vasta gamma di attività, compresa la gestione dei dati personali.

Questo ampliamento dell'accesso ai computer portava con sé un aumento del potere informatico individuale, consentendo a un numero sempre maggiore di persone di raccogliere e elaborare informazioni personali. Tuttavia, questo potere non era sempre trasparente e poteva essere esercitato senza il consenso delle persone interessate, che spesso non comprendevano appieno le modalità tecniche e i meccanismi di gestione dei loro dati. Di fronte a questa concentrazione di potere nelle mani delle istituzioni pubbliche e delle imprese, emergeva una domanda crescente di trasparenza e di regolamentazione della raccolta e del trattamento dei dati personali. I legislatori nazionali rispondevano a questa domanda introducendo normative che bilanciavano le esigenze di gestione delle informazioni con i diritti individuali alla privacy e al corretto trattamento dei dati personali [5].

La prima legge che si è occupata di protezione dei dati personali[6] è la legge del 1970 del Land dell'Assia, contemporaneamente in Francia veniva emanata la prima legge sul diritto alla vita privata, la quale evoluzione nel 1978 ha portato all'istituzione del CNIL (*Commission Nationale de l'Imformatique e des Libertes).* Questa legge, trattando l'informatica come un bene al servizio dei cittadini, ha allargato la tutela alla difesa della vita privata e familiare dall'uso invasivo di queste tecnologie[7]. La legge del Land aveva un obiettivo di stampo politico oltre che di tutela dei cittadini poiché «*con questa Legge si affermava, infatti, una idea di democrazia e di tutela della persona opposta a quella propria della Germania dell'Est, basata invece su forme di controllo vecchie e nuove che in quel Paese si praticavano ampiamente»*[8].

---

[5] Cfr. A. Mantelero, *Il costo della privacy tra valore della persona e ragione d'impresa*, I ed., Milano, 2007, p. 47-54.

[6] La protezione dei dati personali era anche intesa come disciplina e garanzia relativa alla tutela dei dati personali raccolti in banche dati e trattati con metodi automatizzati.

[7] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* cit., p. 59.

[8] V. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* cit*., Ibidem*.

La Germania, però, solo nel 1977 adottò una legge federale per la protezione dei dati personali. Infine, è bene ricordare che nel 1978 la Spagna è stata la prima nazione a riconoscere il diritto alla riservatezza nella sua Costituzione[9].

Il 28 gennaio 1981 il Consiglio d'Europa adotta la Convenzione 108, che rimanda specificamente alla "*protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale*". Nell'art. 1 il rimando è diretto "*in particolare al diritto alla vita privata nei confronti dell'elaborazione automatizzata dei dati di carattere personale che la riguardano*". È importante rilevare che tramite l'art. 2 lett. a) si arriva a dare la prima definizione di dati personali ovvero "*ogni informazione relativa a una persona fisica identificata o identificabile (persona interessata*)"; alla lett. c) si definisce, invece, che "*elaborazione automatizzata comprende le seguenti operazioni effettuate nel loro insieme o in parte grazie a procedimenti automatizzati: registrazione di dati, applicazione ad essi di operazioni logiche e/o aritmetiche, loro modifica, cancellazione, estrazione o diffusione"*[10].

Di eguale importanza sono l'art. 5, che tratta della qualità dei dati, e l'art. 6, che individuava per la prima volta le categorie speciali di dati che è vietato trattare a meno che il diritto interno non prevedesse garanzie adatte, le categorie sono uguali a quelle odierne ovvero tutti quei dati che possono rivelare: l'origine etnica[11], le opinioni politiche, la fede religiosa o qualsiasi credo, lo stato di salute e la vita sessuale, e infine le condanne penali[12].

Giungendo alla parte che più interessa questo elaborato, la Convenzione 108 prevede all'art. 2 lett. d la definizione del "*detentore di una collezione di dati"* come "*la persona fisica o giuridica, la pubblica autorità, il servizio o qualsiasi altro organismo che, secondo la legge nazionale, è competente a decidere quale debba essere la finalità dello schedario automatizzato, quali categorie di dati a carattere personale debbano essere registrate e quali operazioni debbano essere loro*

[9] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* cit., p. 60.
[10] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* cit.,p. 61-62.
[11] La convenzione originariamente faceva riferimento all'origine razziale, si è preferito sostituire quel termine con "etnica" per ovvi motivi.
[12] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* cit.,p. 62.

applicate"[13]. È rilevante notare che all'art. 8 si fa riferimento alla figura del "*responsabile della collezione"*; in particolare, nella lett. a) "*Ogni persona deve avere la possibilità di: a) conoscere l'esistenza di una collezione automatizzata di dati a carattere personale, i suoi fini principali, nonché l'identità e la residenza abituale o la sede principale del responsabile della collezione" [14]*. Si fa cenno anche nell'art. 14 comma 3 lett. b) che recita: "*La richiesta di assistenza deve contenere tutte le indicazioni necessarie, concernenti in particolare: b) la collezione automatizzata di dati a carattere personale al quale si riferisce la richiesta o il detentore di tale collezione di dati*"[15]. Che si chiami detentore o responsabile questa convenzione faceva riferimento a un solo soggetto che possiamo oggi riconoscere nel titolare del trattamento, siccome questa convenzione era stata attuata per regolare solamente i trattamenti automatizzati, che erano quelli che destavano più preoccupazione in quel momento, si può affermare che è stato ritenuto sufficiente prevedere una sola figura che decidesse in merito al cosiddetto casellario automatizzato [16].

1.2 **La direttiva 95/46/UE**

1.2.1 *Premessa. Come si è giunti a questa direttiva e un primo sguardo generale.*

Dal concetto di privacy come "*diritto di essere lasciati soli"* si può affermare che in quegli anni c'è stata una netta evoluzione e la privacy ha acquisito una definizione più dinamica, di pari passo con l'evoluzione tecnologica e culturale. Nonostante questa prima definizione rimanga ancora oggi per determinati aspetti coerente, già in quegli anni aveva perso il suo valore universale poiché il concetto di privacy si può dire che fosse approssimabile a "*il diritto di mantenere il controllo sulle proprie informazioni*". Di conseguenza il concetto di privato si iniziò ad estendere a tutte quelle situazioni che potevano essere tradotte in informazioni e quindi comunicabili

[13] STCE108 Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, https://rm.coe.int/1680078c45 .
[14] Vedi *Ibidem.*
[15] Vedi *Ibidem.*
[16] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* cit., p. 197.

verbalmente o meno, in quest'ottica privato e segreto non coincidono, il privato diventa personale e non obbligatoriamente segreto, semplicemente il soggetto ha il diritto ad avere il controllo sull'informazione personale. Quindi il soggetto che detiene il diritto alla privacy non esige più meramente la segretezza dell'informazione, ma può essere tutelato tramite una "*circolazione controllata*" di tale informazione[17].

In quegli si è assistito a uno sviluppo informatico e socio-economico, che ha evidenziato l'obsolescenza delle impostazioni normative precedentemente adottate. Queste impostazioni erano sostanzialmente concepite facendo riferimento al contesto storico degli anni Ottanta, quando la società non era ancora completamente immersa nell'era dell'informazione, in cui la gestione informatizzata dei dati si affiancava alla loro circolazione sulle reti telematiche. Questo scambio incessante di informazioni divenne essenziale per la vita economica e pubblica, trasformando l'informazione in uno dei beni primari e delle risorse principali di ogni sistema produttivo e non. Con l'aumento del valore aggiunto costituito dai servizi accessori alla produzione e vendita dei beni, che implicavano necessariamente la gestione di dati personali, la raccolta di informazioni sui contraenti e potenziali acquirenti divenne un'attività funzionale alla gestione d'impresa. L'aumento del valore delle informazioni personali ha reso necessario riconoscere pienamente all'individuo la possibilità di gestire queste informazioni come una nuova forma di ricchezza personale. Ciò implica che ogni individuo debba poter decidere come gestire i propri dati e se acconsentire o meno al loro utilizzo da parte di operatori economici, e a quali condizioni.

In risposta a queste esigenze, la disciplina dei dati personali ha subito un'evoluzione, verso un nuovo modello incentrato sul consenso al trattamento dei dati da parte dell'interessato, a partire dalla metà dell'ultimo decennio del secolo scorso. Questi sono i principi e le scelte di politica del diritto che sembrano caratterizzare l'ultima fase delle legislazioni europee in materia di protezione dei dati, conformemente alle linee guida stabilite dalla direttiva comunitaria 95/46/CE adottata nel 1995. In questa normativa, il consenso dell'interessato diventa uno dei punti cardine nel difficile equilibrio tra tutela della persona e sviluppo delle banche

[17] Cfr. S. Rodotà, *Tecnologie e diritti*, I ed., Bologna, 1995, 101-103.

dati, dove la protezione dell'individuo è considerata fondamentale per il corretto funzionamento del mercato comune dell'Unione[18]

Avendo riflettuto sul concetto di privacy è ora utile fare un'ulteriore passo in avanti trattando situazione di quel momento in Europa per comprendere cosa ha spinto nei fatti ad arrivare alla Direttiva 95/46. La Comunità Europea non si è mai dotata di forme di regolazione in merito alla protezione dei dati personali fino al 1995, anno in cui è stata adottata la Direttiva 95/46/CE *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.* Per comprendere il motivo per cui si è deciso di emanarla nel 1995, è necessario fare una breve digressione relativa al Trattato di Maastricht del 7 febbraio 1992. Entrato ufficialmente in vigore il 1° novembre 1993, grazie all'avvio della politica monetaria unica, questo Trattato è stato fondamentale per agevolare l'unificazione tedesca successiva ai fatti del muro di Berlino del 1989 e alla dissoluzione dell'URSS avvenuta nel 1992, poiché grazie all'unione che ha creato tra i Paesi è stato possibile che tutti ne diedero il pieno consenso, prima di tutto la Francia che sarebbe stato quello più difficile da convincere [19].

Questo Trattato diede inizio a tre processi: la costituzione stessa dell'Unione Europea; l'impegno alla piena attuazione del Mercato Unico nell'ambito della Comunità Europea; il processo di allargamento dell'Unione, tradotto in norme dal Trattato di Amsterdam firmato il 22 ottobre 1997 ed entrato in vigore il 1° maggio 1999, stabilendo le regole fondamentali per gli Stati che entrano nell'Unione [20].

L'abbattimento dei controlli doganali relativo al Trattato di Maastricht e dei controlli di frontiera anche alle persone relativo alla Convenzione di Schengen, che fu integrata al Trattato di Maastricht nel 1999 tramite il Trattato di Amsterdam, costituirono due problemi per la protezione dei dati personali[21]: «*l'abbattimento delle dogane per le merci […] aveva un effetto inevitabilmente limitato dal fatto che per ogni Paese, fornitore o destinatario della merce, potessero valere regole diverse*

[18] Cfr. A. Mantelero, *Il costo della privacy tra valore della persona e ragione d'impresa* cit., p.57-60.
[19] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* cit., p. 64.
[20] Cfr. *Ibidem.*
[21] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* cit., p. 65.

relativamente all'uso dei dati personali collegati agli scambi»[22]. Per questo motivo, nel 1990, si avviarono le trattative per arrivare a una normativa europea uniforme in materia, concludendosi appunto nel 1995 con la suddetta direttiva, che, però, ebbe uno scopo di armonizzazione delle leggi già vigenti nei Paesi firmatari, nel senso che stabiliva dei principi e regole mediamente vincolanti a cui le leggi nazionali dovevano uniformarsi [23].

La conseguenza più grande di questa direttiva fu data dal principio del mutuo riconoscimento, il quale «*consiste nel fatto che in ogni Paese dell'Unione si applica la legge di protezione dati del Paese in cui ha sede lo stabilimento principale del titolare del trattamento»*[24].

In merito al rapporto con i Paesi terzi all'art. 25 si stabiliva che il trasferimento dei dati verso il suddetto Paese terzo era possibile solo se questo aveva un grado di protezione dati alto tanto quanto il Paese europeo da cui sarebbero partiti i dati. Questo comportò non poche difficoltà e soprattutto si può dire che rafforzò una sorta di isolamento dell'Unione tra i propri confini in materia [25].

Questa Direttiva fu un passo importante anche nell'ottica della Convenzione di Schengen, poiché era importante che i Paesi membri armonizzassero le loro leggi in relazione alla Direttiva prima di aderire alla Convenzione, poiché l'abbattimento dei confini materiali passava anche dall'abbattimento di quelli immateriali conseguente alla Direttiva. Questa Direttiva è quindi arrivata con un tempismo giusto per essere d'aiuto alla Convenzione di Schengen poiché senza si sarebbe verificato un vuoto normativo in merito alla circolazione dei dati nell'Unione [26] .

---

[22] V. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* cit.,*Ibidem.*

[23] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* cit., *Ibidem.*

[24] V. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* cit.*,* p. *66.*

[25] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* cit., *Ibidem.*

[26] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* cit., p. *67.*

1.2.2 *Il contenuto della direttiva in relazione ai soggetti del trattamento*

Nella Direttiva 95/46/CE non c'è una sezione dedicata interamente ai soggetti del trattamento come avverrà nel GDPR, ma questi compaiono via discorrendo negli articoli e vengono esplicati all'art.2 in cui vengono date delle prime definizioni. Infatti all'art.2 lett. d) vi è scritto "*«responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali. Quando le finalità e i mezzi del trattamento sono determinati da disposizioni legislative o regolamentari nazionali o comunitarie, il responsabile del trattamento o i criteri specifici per la sua designazione possono essere fissati dal diritto nazionale o comunitario;"* e alla lett. e) "*«incaricato del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che elabora dati personali per conto del responsabile del trattamento;*"[27].

Analizzando la Direttiva, è rilevante parlare degli articoli 10 e 11 che regolano il diritto degli interessati a essere informati sul trattamento, con differenze tra dati raccolti presso la persona interessata (art. 10) e dati non raccolti presso la persona interessata (art. 11), in particolare hanno il diritto a conoscere le seguenti informazioni: l'identità del responsabile del trattamento ed eventualmente del suo rappresentante; le finalità del trattamento cui sono destinati i dati; ulteriori informazioni riguardanti quanto segue: i destinatari o le categorie di destinatari dei dati, se rispondere alle domande è obbligatorio o volontario, nonché le possibili conseguenze di una mancata risposta, se esistono diritti di accesso ai dati e di rettifica in merito ai dati che la riguardano [28].

Successivamente è giusto far riferimento al diritto di accesso regolato dall'art. 12 che sostanzialmente impone al responsabile, in caso che l'interessato ne richieda, di dare accesso alle seguenti informazioni: la conferma dell'esistenza o meno di trattamenti di dati che la riguardano, e l'informazione almeno sulle finalità dei trattamenti, sulle categorie di dati trattati, sui destinatari o sulle categorie di

---

[27] Direttiva 95/46/CE, consultata al link: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX%3A31995L0046 .

[28] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* cit.,p. 86-87.

destinatari cui sono comunicati i dati; la comunicazione in forma intelligibile dei dati che sono oggetto dei trattamenti, nonché di tutte le informazioni disponibili sull'origine dei dati; la conoscenza della logica applicata nei trattamenti automatizzati dei dati che lo interessano, per lo meno nel caso delle decisioni automatizzate di cui all'articolo 15, paragrafo 1. Inoltre, questo articolo regola anche il diritto alla cancellazione, rettifica o congelamento dei dati in caso di violazione della direttiva e della sua comunicazione ai terzi che hanno avuto accesso ai dati[29].

L'art. 16 che regola la riservatezza dei trattamenti impone all'incaricato di non elaborare i dati senza l'istruzione del responsabile o per obblighi legali; successivamente l'art. 17 è dedicato alla sicurezza dei trattamenti, si può dire che è un'apripista per quella che sarà l'architettura del GDPR in cui si dedica molto spazio alle misure di sicurezza da adottare da parte dei soggetti del trattamento. In questo articolo, oltre che imporre di utilizzare le più rigorose misure di sicurezza, si regola il rapporto tra responsabile e incaricato tramite un contratto che prevede che l'incaricato operi solo sotto le istruzioni del responsabile e che si impegni a rispettare le misure di sicurezza espletate al primo paragrafo dell'articolo[30].

Gli articoli dal 18 al 21 sono interamente dedicati all'obbligo di notificazione da parte del responsabile del trattamento all'autorità di controllo competente. All'art. 18 veniva appunto inizialmente esplicato l'obbligo di notificazione di trattamenti interamente o parzialmente automatizzati all'autorità garante, mentre per i trattamenti non automatizzati prevede la possibilità di esonero o semplificazione della procedura in alcuni casi (comma 5) così come al comma 6 che richiama l'art. 8 lett.d per i trattamenti effettuati da "*qualsiasi organismo che non persegua scopi di lucro e rivesta carattere politico, filosofico, religioso o sindacale, nell'ambito del suo scopo lecito e a condizione che riguardi unicamente i suoi membri o le persone che abbiano contatti regolari con la fondazione, l'associazione o l'organismo a motivo del suo oggetto e che i dati non vengano comunicati a terzi senza il consenso delle*

[29] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* cit., p.*89.*

[30] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* cit*., p. 95-96.*

persone interessate"[31]; successivamente sono elencate le condizioni per essere esonerati da quest'obbligo o comunque ottenerne una semplificazione ovvero: in primis solo per quelle categorie di trattamento, che considerati i dati in oggetto, non pregiudichino i diritti e la libertà dell'interessato si prevede si specificare semplicemente le finalità del trattamento, i tipi di dati trattati, le persone coinvolte, i destinatari dei dati e il periodo di conservazione e/o per quei trattamenti che in cui viene nominato un responsabile della protezione dei dati per garantire la conformità alle normative nazionali e che tenga un registro dei trattamenti per proteggere i diritti e le libertà delle persone interessate.

All'art. 19 vengono esplicate un minimo di informazioni che devono essere presenti nella notifica a discrezionalità degli Stati membri: il nome e l'indirizzo del responsabile del trattamento, le finalità del trattamento, le categorie di persone interessate e i dati trattati, i destinatari dei dati, i trasferimenti di dati verso paesi terzi e una descrizione generale delle misure adottate per garantire la sicurezza del trattamento; la discrezionalità è lasciata anche per definire le modalità di notifica sia di queste informazioni che di eventuali mutamenti. Successivamente si dispone un controllo preliminare da parte dell'autorità di controllo o dell'eventuale persona nominata per la protezione dei dati, anche qui è lasciata discrezionalità agli stati membri per definire gli eventuali trattamenti che sono fonte di rischio per i diritti e le libertà delle persone (art.20). Infine, all'art. 21 è regolata la pubblicità dei trattamenti e la necessità di adottare misure per assicurarla. Gli Stati membri sono tenuti a garantire che l'autorità di controllo mantenga un registro dei trattamenti dati notificati. Questo registro deve contenere almeno le informazioni specificate nell'articolo 19. Inoltre, il registro deve essere accessibile a chiunque desideri consultarlo[32].

[31] Direttiva 95/46/CE, consultata al link: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX%3A31995L0046 .

[32] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* cit., p. *98 s.*

1.2.3 *La Legge del 31 dicembre 1996, n.675*

Dopo questa panoramica sulla Direttiva 95/46 è utile richiamare come il legislatore italiano abbia trasposto tale normativa nel nostro ordinamento. Lo Stato italiano ha recepito la direttiva promulgando la Legge 31 dicembre 1996, n. 675 dal titolo "*Tutela delle persone e di altri soggetti rispetto al trattamento di dati personali*". In questa legge i due soggetti già citati sono definiti in modo diverso, sono chiamati responsabile e titolare del trattamento, il primo corrisponde all'incaricato del trattamento che compare nella direttiva, e il secondo coincide con il responsabile; tutto ciò con sfumature diverse che verranno analizzate[33]. Anche in questa legge l'inizio è dedicato alle definizioni che si trovano all'art.1 lett. e): "*per "titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza;*" e alla lett. f): "*per "responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;*"[34].

Al responsabile è dedicato solo l'art. 8, che però ne definisce più i compiti professionali e non introduce uno schema di obblighi e diritti in modo preciso come si è configurato per il titolare. Inoltre, l'art. 8, terzo comma, recita: "*Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti*"[35]. Da qui sembrerebbe che il responsabile debba essere una persona fisica, mentre nell'art. 1 si era data una definizione completa in cui si integravano anche persone giuridiche, enti e PA. Da qui si evince la presenza di un'antinomia, che però potrebbe risolversi col fatto che questa persona fisica facesse parte della tale associazione riconosciuta e non, ente o PA. Sono evidenti altri dubbi derivanti dal rapporto tra titolare e responsabile, poiché all'art. 1 lett. e) si parla di "*preposizione"* del responsabile da parte del titolare lasciando intendere una

[33] Cfr. V. Cuffaro, V. Ricciuto, *La disciplina del trattamento dei dati personali*, I ed., Torino, 1997, 104.
[34] Legge 31 dicembre 1996, n.675, consultata al link: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/28335 .
[35] *Ibidem.*

piena delega mentre l'art. 8 fa riferimento a un rapporto visibilmente gerarchico e verticale[36].

Risulta possibile affermare che in questo caso il legislatore ha cercato di ricomprendere più casi possibili e per cui va interpretata in maniera estensiva, da qui ne deriva una mancanza di precisione. Inoltre, ciò che risulta evidente è che il responsabile non risultava portare un interesse proprio, se per il titolare e l'interessato erano ben chiari e tecnicamente opposti, ovvero la riservatezza per il primo e il vantaggio economico per il secondo. Dall'art. 8 sembra trasparire che il responsabile fosse una figura meramente operativa a cui più che obblighi e diritti vengono impartiti dei doveri[37].

Parlando del titolare è giusto osservare l'equiparazione tra soggetto pubblico e soggetto privato, che è molto importante visto che la Pubblica Amministrazione senza dei regolamenti poteva mettere in atto raccolte di dati molto invasive per i cittadini. È giusto poi notare che nella legge erano poi presenti delle distinzioni: questa normativa, ai sensi dell'art. 4, non si applicava ad alcuni trattamenti se tali dati da parte di soggetti pubblici diversi dagli enti pubblici economici non era soggetto al consenso dell'interessato, sempre che fosse a norma dell'art. 27 e, quindi, effettuato per funzioni istituzionali, nei limiti stabiliti da leggi e regolamenti. Un'ultima differenza è data dal fatto che per iniziare un trattamento ai soggetti privati bastava dare comunicazione al Garante, mentre per i soggetti pubblici è necessario che sia previsto da leggi e regolamenti[38].

È rilevante osservare come questa normativa italiana si avvicinasse alle cosiddette "*leggi di seconda generazione*", se le prime leggi sulla protezione dei dati personali permettevano solo i trattamenti autorizzati ed esplicitati dalle leggi, queste di seconda generazione hanno una struttura che permette tutti i trattamenti tranne quelli espressamente vietati[39].

[36] Cfr. Cuffaro, Ricciuto, *La disciplina del trattamento dei dati personali* cit., p.105.
[37] Cfr. Cuffaro, Ricciuto, *La disciplina del trattamento dei dati personali* cit., 106-107.
[38] Cfr. Cuffaro, Ricciuto, *La disciplina del trattamento dei dati personali* cit., 111,112.
[39] Cfr. Cuffaro, Ricciuto, *La disciplina del trattamento dei dati personali* cit., 114-115.

1.2.4 *Il D.Lgs.196/2003*

La legge 675/96 fu il primo grande passo per recepire questa direttiva, ma la definitiva emanazione del Codice italiano in materia di protezione dei dati personali arrivò con il D.Lgs 196/2003[40], che, per quel che concerne questa ricerca, introdusse due novità quantomeno rilevanti. La prima novità è rappresentata dall'allargamento della figura del titolare (ai sensi dell'art. 4, lett. f, "*"titolare", 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 finalita', alle modalita' del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;*")[41]. In realtà, non è una novità che si è inventato il legislatore italiano, poiché, come già detto precedentemente, la Direttiva 95/46 prevedeva all'art. 2, lett. d) che diversi soggetti giuridici potessero assumere il ruolo di titolari del trattamento, ma solamente a condizione di una specifica base giuridica che lo consenta e di unala finalità unica e condivisa. L'evoluzione delle tecnologie ha poi portato a chiedersi se fosse rispettata questa parte, poiché con il *boom* dell'*online* sembravano svilupparsi sempre di più situazioni in cui si presentavano soggetti diversi con finalità diverse che di fatto erano contitolari[42].

La seconda novità introdotta da questo Decreto è rappresentata dall'art. 4 lett. h), secondo cui sono *"incaricati" "le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;*"[43]. La figura dell'incaricato è frutto del legislatore italiano, poiché non era previsto dalla Direttiva 95/46, e fa riferimento ai soggetti a cui vengono commissionati i compiti e le mansioni di secondo livello dal titolare o dal responsabile. Si può notare anche solo leggendo il paragrafo relativo alla Direttiva che il termine *incaricato* nel diritto europeo è stato

[40] Per il resto del paragrafo si parlerà di esso con la locuzione Codice Italiano.
[41] Consultato in Gazzetta Ufficiale al link https://www.gazzettaufficiale.it .
[42] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* cit., 201.
[43] Consultato in Gazzetta Ufficiale al link https://www.gazzettaufficiale.it .

utilizzato per definire quello che in Italia è chiamato responsabile[44]. All'art. 30 si specificava che:

"*1. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.*

2. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima".

Questa figura fu bersaglio di critiche a livello europeo e italiano, sia per i motivi già detti precedentemente che per la troppa burocrazia che derivava dalla normazione così dettagliata di questa figura. Inoltre, in alcuni casi rendeva difficile capire se un incaricato nominato dal titolare fosse appunto incaricato o responsabile[45].

1.3 **GDPR: lo stato attuale dei soggetti del trattamento**

Prima di addentrarsi nel GDPR è bene far riferimento a due passaggi importanti: l'approvazione della Carta di Nizza il 7 dicembre 2000 e l'approvazione del Trattato di Lisbona il 1 dicembre 2009. La Carta di Nizza (poi incorporata nel Trattato di Lisbona) riconosce all'art. 8 la protezione dei dati personali come diritto fondamentale e ancor più rilevante l'art. 16 del TFUE dichiara l'Unione competente a legiferare in materia di protezione dei dati personali. Su questo flusso gli anni precedenti al Regolamento sono stati ricchi di pareri e aggiustamenti fino a quando non si è reso necessario il GDPR[46].

Col passare del tempo la Direttiva 95/46 si è sempre dimostrata più inadeguata, soprattutto a causa dell'evoluzione del mondo digitale, giungendo al culmine quando si aprì la discussione sul futuro della protezione dei dati personali nel 2010, che si tradusse nel "Pacchetto di protezione dati" presentato dalla Commissione il 25

---

[44] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* cit., p. 205.

[45] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* cit., p. 206.

[46] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* cit., p. *140-141.*

gennaio 2012, culminata dopo anni di lavoro alla formulazione del Regolamento il 17 dicembre 2015[47]. Qui di seguito sono spiegate le peculiarità del Regolamento riguardo ai soggetti del trattamento.

1.3.1 *Titolare del trattamento (controller) e responsabile del trattamento (processor)*

Il *focus* di questo regolamento nell'ambito dei soggetti è la loro responsabilità ovvero il c.d. principio di *accountability*, che può essere analizzato da un lato oggettivo e da uno soggettivo. *In primis*, ci sono grandi novità dal lato delle misure e tecniche imposte al titolare poiché il trattamento risulti conforme al Regolamento; in particolare, l'approccio che devono tenere imprese ed enti pubblici risulta modificato a partire dal *risk based approach*. Dal lato soggettivo, quindi riguardo ai ruoli e ai compiti dei veri soggetti facenti parte la catena del trattamento, c'è continuità con la Direttiva precedente, mantenendo inalterate le figure di titolare e responsabile. La novità è, infatti, nella dettagliata esplicazione di compiti e limiti di questi soggetti[48].

Il termine *accountability*, originariamente di derivazione anglosassone e traducibile in italiano come *responsabilità* o *obbligo di rispondere*, è stato reso più appropriatamente con il termine *responsabilizzazione* dal Legislatore nazionale. Questa scelta riflette l'essenza del principio, che impone al titolare del trattamento di adottare misure conformi alla normativa privacy e di dimostrare di averle attuate. Un corollario della responsabilizzazione è il principio della minimizzazione dei dati personali, secondo il quale il titolare deve utilizzare i dati raccolti solo per gli scopi specifici per i quali sono stati richiesti. Questo concetto non è nuovo nel sistema italiano, poiché il Codice Italiano prevedeva già il principio di necessità del trattamento dei dati. La responsabilizzazione dei titolari del trattamento e il principio della minimizzazione dei dati personali sono fondamentali per garantire una

[47] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo* cit*., 36 s.*

[48] Cfr. S. Calzolaio, L. Ferola, V. Fiorillo, E. A. Rossi, M. Timiani, *La responsabilità e la sicurezza del trattamento* in L. Califano, C. Colapietro (a cura di), *Innovazione tecnologica e valore della persona: il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, I ed., Napoli, 2017, 142-143.

protezione efficace dei dati personali e rispondono alla necessità di adattare la normativa alla crescente complessità delle attività di trattamento dei dati[49].

Il titolare del trattamento (controller).

I soggetti del trattamento, come nei casi precedenti, vengono introdotti nell'articolo 4 (rubricato "definizioni"); il n. 7 dedicato al titolare recita: "*«titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri*"[50]. Questa definizione è praticamente uguale a quella nella Direttiva 95/46, già citata in precedenza, ma sensibilmente diversa è la disciplina, visto che in questo Regolamento è dedicato l'intero Capo IV solo agli obblighi di titolare e responsabile [51].

L'attuale definizione mette in evidenza un tratto distintivo della figura, che si ritrova anche nei precedenti testi legislativi: la portata della norma è massimizzata, consentendo a persone fisiche o giuridiche, enti pubblici o privati di rivestire il ruolo di titolare. In sintesi, chiunque può essere titolare del trattamento. Bisogna specificare una limitazione parziale nell'applicazione del Regolamento 2016/679. Esso non si applica al trattamento di dati personali effettuato da un individuo nell'ambito di attività puramente personali o domestiche (non legate a un'attività commerciale o professionale). Tuttavia, ciò non esclude affatto che il Regolamento sia applicabile al soggetto che mette a disposizione i mezzi per il trattamento dei dati personali nell'ambito di queste attività personali o domestiche[52].

Per chiarire la posizione del titolare del trattamento è utile far riferimento al Parere n. 1 del 16 settembre 2010 del gruppo art. 29, in particolare nella parte in cui

---

[49] Cfr. F. Brizzi, *il GDPR in ambito giudiziario: fino a che punto può spingersi l'accountability?* in Ius Penale Gfl, 11.12.2018, consultato il 22.04.2024.

[50] GDPR consultato al link: GDPR

[51] Cfr. F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: il Regolamento europeo 2016/679,* I ed., Torino, 2016, 56.

[52] Cfr. D. Farace, *Il titolare e il responsabile del trattamento* in V. Cuffaro, R. D'Orazio, V. Ricciuto, *I dati personali nel diritto europeo,* I ed., Torino, 2019, p. 734.

viene precisato che chiunque prenda decisioni in riferimento alla determinazione delle finalità e dei mezzi del trattamento diventi titolare di esso, in modo che chiunque vada oltre i suoi compiti risponda successivamente delle conseguenze di ciò[53].

A questo proposito risulta utile citare il caso in cui col provvedimento n. 293 del 13 maggio 2015 il Garante per la Protezione dei dati ha sanzionato la società I. Spa condannandola al pagamento di 40000 euro. Nel caso preso in esame, la società I. Spa è stata sanzionata per trattamenti di dati personali non autorizzati, che coinvolgevano l'attivazione di schede telefoniche senza il consenso dei titolari. La società ha contestato l'attribuzione del ruolo di titolare del trattamento, sostenendo di agire come responsabile in ottemperanza alle istruzioni del vero titolare, la compagnia telefonica. Il Tribunale di Milano ha respinto l'opposizione della società confermando la qualifica di titolare del trattamento. La società ha quindi presentato ricorso in Cassazione, argomentando che il Tribunale avesse erroneamente attribuito la qualifica di titolare anziché di responsabile; il ricorso è stato rigettato. Come precedentemente detto, il titolare è il soggetto che determina le finalità e i mezzi del trattamento dei dati, mentre il responsabile tratta i dati per conto del titolare, attenendosi alle istruzioni di quest'ultimo. Il caso evidenzia l'importanza della corretta definizione dei ruoli nel trattamento dei dati personali e della necessità che il responsabile operi sotto la supervisione e le istruzioni del titolare. Se il responsabile eccede i suoi poteri o non segue le istruzioni, può essere considerato titolare a tutti gli effetti e ritenuto responsabile delle violazioni delle normative sulla protezione dei dati[54].

La definizione normativa chiarisce limpidamente i tratti fondamentali della figura: *autonomia* e *necessità*. *Autonomia*, perché il titolare, nel rispetto degli obblighi legali, determina sia le finalità che i mezzi del trattamento. Attraverso i propri atti, designa i soggetti subordinati e ne regola l'operato. Per gli enti pubblici, la determinazione delle finalità del trattamento è differente rispetto ai soggetti privati.

[53] Cfr. E. Tuccari, *I soggetti del trattamento* in G. Magri, S. Martinelli, S. Thobani (a cura di), *Manuale di diritto privato delle nuove tecnologie*, I ed., Torino, 2022, 174.

[54] Cfr. R. Settimio, *Obblighi e responsabilità dei soggetti del trattamento: titolare e responsabile a confronto*, in Giustiziacivile.com, 18.03.2022, consultato il 10.03.2024.

La *necessità* deriva dal fatto che, salvo eccezioni previste dalla legge, in ogni trattamento di dati personali di individui fisici è essenziale l'identificazione di un titolare. A differenza di altre figure, la presenza del titolare non è facoltativa, ma sempre imprescindibile[55].

Le linee guida del Comitato europeo per la protezione dei dati del 7 luglio 2020 sono importanti da citare poiché danno un chiarimento riguardo ai mezzi del trattamento, distinguendoli tra essenziali e non. Riassumendo, si può dire che i mezzi essenziali si riferiscono alle finalità come il tipo di dati personali trattati, la durata del trattamento, le categorie dei destinatari e le categorie dei soggetti di dati. Questi mezzi essenziali sono riservati al Titolare, mentre quelli non essenziali possono essere decisi anche dal responsabile e riguardano aspetti più pratici come la scelta di un particolare *hardware* o *software*[56].

Inoltre, si può dire che «*oggi è parimenti certo che il titolare del trattamento, il più delle volte è una persona giuridica, ovvero un'entità pubblica o privata, in cui la persona fisica "legale rappresentante" funge solo da portavoce dei suoi interessi, ma senza che si possa attribuire a lui individualmente alcuna responsabilità*»[57].

Il titolare ha una vasta gamma di obblighi, diritti, poteri e facoltà che gli sono assegnati. Questi doveri variano e possono essere distinti in obblighi generali e specifici, che a loro volta possono essere classificati in diverse categorie.

Prima di tutto, è importante considerare gli obblighi generali che il titolare deve rispettare, come stabilito nell'articolo 5, paragrafo 1, del Regolamento 2016/679. Questo articolo stabilisce i principi fondamentali che guidano il trattamento dei dati personali. Essi comprendono la necessità di garantire la liceità, la correttezza e la trasparenza nel trattamento dei dati, così come la limitazione del trattamento solo a fini specifici e legittimi. Inoltre, il titolare deve assicurarsi che i dati trattati siano adeguati, pertinenti e limitati a quanto necessario per il conseguimento delle finalità previste. È altresì obbligatorio mantenere l'accuratezza dei dati e aggiornarli se necessario, oltre a conservarli solo per il tempo strettamente necessario. Infine, il

---

55 Cfr. Farace, *Il titolare e il responsabile del trattamento* cit., p. 735 s.
56 Cfr. Tuccari, *I soggetti del trattamento* cit. p. 175.
57 V. Calzolaio, Ferola, Fiorillo, Rossi, Timiani, *La responsabilità e la sicurezza del trattamento* cit., p. 145.

titolare è tenuto a garantire l'integrità e la riservatezza dei dati, adottando adeguate misure di sicurezza per proteggerli da accessi non autorizzati o da utilizzi impropri.

Questi principi costituiscono la base su cui il titolare deve basare le proprie azioni nel trattamento dei dati personali, garantendo il rispetto dei diritti degli interessati e l'adempimento degli obblighi legali previsti[58].

Successivamente sono trattati gli obblighi di informazione e comunicazione verso l'interessato, che sono molto complessi. Il titolare deve prima di tutto adottare tutte le misure adeguate per fornire le informazioni necessarie, come richiesto dagli articoli 13-14 del Regolamento 2016/679. Se il trattamento dei dati si basa sul consenso dell'interessato, il titolare deve ottenere questo consenso prima di procedere. È poi responsabile di dimostrare di aver ottenuto il consenso, come specificato nell'articolo 7, paragrafo 1 del Regolamento.

Quando si tratta di dati personali di minori, il titolare deve fare ogni ragionevole sforzo per verificare che il consenso sia stato ottenuto o autorizzato da chi esercita l'autorità genitoriale, come stabilito nell'articolo 8, paragrafo 2 del Regolamento. Oltre agli obblighi di informazione, il titolare ha molti doveri di comunicazione verso l'interessato, descritti negli articoli 15-22 e 34 del Regolamento 2016/679. Deve anche facilitare l'esercizio dei diritti dell'interessato, fornendo informazioni e comunicazioni gratuitamente e in tempi stabiliti dal Regolamento. Queste comunicazioni devono essere concise, trasparenti, comprensibili e facilmente accessibili, con linguaggio semplice e chiaro, soprattutto se rivolte ai minori. La comunicazione di violazioni dei dati, come previsto nell'articolo 34 del Regolamento, è una delle comunicazioni principali che il titolare deve fare all'interessato. Inoltre, sono previste specifiche comunicazioni all'Autorità Garante, come indicate nell'articolo 36, paragrafo 3 del Regolamento[59].

L’art. 24 introduce il fatto che il titolare, oltre ad adottare le misure tecniche ed organizzative volte ad assicurare una tutela adeguata, deve essere in grado di dimostrarlo, utilizzando anche i codici di condotta come suo strumento a favore, di questi si parlerà successivamente. Ciò che ne deriva è una figura del titolare con un

[58] Cfr. Farace, *Il titolare e il responsabile del trattamento* cit., p. 741 s.
[59] Cfr. Farace, *Il titolare e il responsabile del trattamento* cit., pp. 744, 745.

ruolo proattivo per rispettare le regole e dimostrarne il rispetto. La novità più rilevante è data dal tema dell'ambito di applicazione territoriale che tramite l'art. 3 e il considerando 36 in base ai quali a determinate condizioni può essere chiamato in causa anche un titolare con stabilimento al di fuori del territorio UE. Questa novità è diretta alle compagnie internazionali che operano nel settore delle comunicazioni elettroniche in modo da tutelare i destinatari dei servizi a compimento di un percorso nato nella Corte di Giustizia con le sentenza *Google Spain* e *Weltimmo*[60].

Il titolare e il responsabile del trattamento devono implementare adeguate misure tecniche e organizzative per garantire un livello di sicurezza proporzionato al rischio. Il titolare deve mantenere un registro delle attività di trattamento, conforme all'articolo 30, paragrafo 1, del Regolamento 2016/679, sia in forma scritta che elettronica. Una violazione dei dati personali è definita come una violazione della sicurezza che comporta la distruzione, perdita, modifica, divulgazione non autorizzata o accesso non autorizzato ai dati personali. In caso di violazione, il titolare deve documentarla accuratamente, valutarne le implicazioni e adottare le misure necessarie per risolverla. Se la violazione presenta rischi per i diritti e le libertà delle persone fisiche, deve notificarla all'autorità di controllo competente entro 72 ore. Se il rischio è elevato, deve anche comunicare la violazione all'interessato senza indugi, fornendo tutte le informazioni pertinenti. In sintesi, gli obblighi del titolare in caso di violazione si dividono in tre categorie: obblighi generici al verificarsi di qualsiasi violazione, obblighi specifici per violazioni gravi e obblighi per violazioni particolarmente gravi[61].

Risulta ugualmente importante parlare dell'art. 56, in particolare il primo comma il quale stabilisce che l'autorità di controllo dello Stato dove si trova lo stabilimento principale o unico del titolare del trattamento, in caso di trattamenti transfrontalieri sarà l'autorità capofila della procedura descritta dall'altrettanto rilevante art. 60. Si nota l'impronta responsabilizzante dal fatto che è il titolare che deve indicare dove si trova il suo stabilimento principale e quindi sotto che Autorità agire, ma se si dovesse ravvisare che in tale stabilimento non ci sono vere e proprie attività gestionali o

[60] Cfr. Calzolaio, Ferola, Fiorillo, Rossi, Timiani, *La responsabilità e la sicurezza del trattamento* cit., pp. *145-147.*

[61] Cfr. Farace, *Il titolare e il responsabile del trattamento* cit., pp. 745-746.

decisionali rispetto al trattamento dei dati personali, le Autorità di controllo del caso si occuperanno di individuare l'Autorità Capofila, in modo da evitare il c.d. *forum shopping*[62].

Il Regolamento 2016/679 richiede al titolare di cooperare con l'Autorità Garante in due modi distinti. In primo luogo, deve rispettare una serie di obblighi specifici definiti dal Regolamento, come mettere a disposizione il registro delle attività di trattamento, pubblicare i dati di contatto del responsabile della protezione dei dati e fornire tutte le informazioni richieste dall'Autorità. Inoltre, deve consentire l'accesso agli ambienti e agli strumenti di trattamento dei dati. In caso di necessità, il titolare deve collaborare anche con l'Autorità capofila e con il Comitato europeo per la protezione dei dati. Il secondo tipo di obblighi di cooperazione è previsto dall'articolo 31, che impone al titolare, al responsabile e al loro rappresentante di cooperare con l'Autorità quando richiesto. Questo obbligo specifico di cooperazione sorge non appena l'Autorità fa richiesta. Se non si applicano i casi specifici previsti da altri articoli, l'Autorità può sempre richiedere al titolare di collaborare per situazioni specifiche. Inoltre, il titolare è tenuto a cooperare con gli organismi di certificazione e con i soggetti da lui designati, come stabilito nell'articolo 43 del Regolamento 2016/679[63].

Il titolare del trattamento ha meno diritti e poteri rispetto agli obblighi imposti, suggerendo che deve considerare anche gli interessi degli altri. Tuttavia, ha il diritto alla cooperazione degli altri. Questa collaborazione è reciproca: il titolare ha il diritto di essere assistito e informato dal responsabile del trattamento, così come dal responsabile della protezione dei dati. Il titolare può decidere le finalità e i mezzi del trattamento, nonché scegliere i soggetti a cui affidare mansioni e compiti relativi al trattamento dei dati. Può anche trasferire dati personali verso altri Paesi o organizzazioni internazionali, stipulare contratti con altri titolari per la contitolarità e determinarne le condizioni. Tuttavia, non ha il potere di disporre dei dati basandosi unicamente sulla sua qualità formale di titolare[64].

---

[62] Cfr. Calzolaio, Ferola, Fiorillo, Rossi, Timiani, *La responsabilità e la sicurezza del trattamento* cit., p. *147.*

[63] Cfr. Farace, *Il titolare e il responsabile del trattamento* cit., pp.747-748.

[64] Cfr. Farace, *Il titolare e il responsabile del trattamento* cit.*,* p. *749.*

Nella definizione citata inizialmente, come nella Direttiva 95/46, è esplicitata la possibilità di avere più titolari per lo stesso trattamento, ovvero i contitolari. In questa direttiva veniva solo citato nella definizione, mentre nel GDPR è dedicato l'intero articolo 26 per normare questa figura. L'articolo inizia definendo che si ha una contitolarità quando i due soggetti congiuntamente i mezzi e le finalità del trattamento; per il resto, verte tutto sull'accordo interno che devono prendere essi, che stabilisce le loro rispettive responsabilità rispetto agli obblighi verso gli interessati, in particolare da quelli derivanti dagli artt. 13-14 in merito ai diritti dell'interessato e alle comunicazioni delle informazioni, sempre che non siano determinate dal diritto dell'Unione o dello Stato membro. Questo accordo deve, inoltre, ripartire i rispettivi ruoli dei contitolari e il loro rapporto con gli interessati e indipendentemente da esso gli interessati possono far valere i propri diritti nei confronti di ciascun titolare[65].

Il responsabile del trattamento (processor)

L'art. 4 GDPR definisce "*«responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*"[66]. Il primo elemento importante è dato dal paragrafo 1 dell'art. 28 GDPR in cui si dice che quando il titolare ritiene di dover nominare un responsabile, deve sincerarsi che sulle garanzie che questo può dare in termini di tecniche e misure organizzative di cui ha bisogno[67].

Prima di addentrarsi nel contesto normativo è doveroso riflettere su quattro caratteri essenziali che definiscono questo soggetto: facoltatività, strumentalità, preposizione e professionalità.

La prima cosa importante da notare è che il responsabile del trattamento non è obbligatorio come il titolare. Anche se facoltativo, spesso viene comunque nominato perché il titolare potrebbe trovare difficile gestire direttamente le attività relative al trattamento dei dati personali, considerando gli obblighi legali e le responsabilità

---

[65] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: il Regolamento europeo 2016/679* cit., p. 56.

[66] GDPR consultato al link: GDPR

[67] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: il Regolamento europeo 2016/679* cit., p. 58.

connesse. Il titolare può svolgere tutto da solo o con l'aiuto di collaboratori, senza nominare un responsabile, ma può anche incaricare uno o più soggetti per questo ruolo. Un aspetto cruciale del ruolo del responsabile del trattamento è la sua natura strumentale: il responsabile gestisce dati personali per conto del titolare del trattamento, non per conto proprio. Con il Regolamento 2016/679, il responsabile deve conformarsi alle finalità del trattamento stabilite dal titolare, che detiene il controllo sulle decisioni fondamentali e sui mezzi impiegati. Il responsabile può agire solo sulla base di istruzioni documentate del titolare; in mancanza di tali istruzioni, non può trattare alcun dato. Questa strumentalità definisce il rapporto tra il responsabile e il titolare: il responsabile deve servire gli interessi del titolare e agire esclusivamente per suo conto.

Il responsabile del trattamento è caratterizzato dalla sua posizione subordinata al titolare. Deve eseguire compiti assegnati dal titolare, seguendo le sue istruzioni e direttive. L'inadempimento alle istruzioni può comportare che il responsabile assuma il ruolo di titolare. Si discute se il responsabile possa essere interno all'organizzazione del titolare o no, poiché il Regolamento europeo presenta ambiguità in merito. Anche se il responsabile non dipende direttamente dal titolare, il suo ruolo dovrebbe comunque essere caratterizzato dalla subordinazione. Anche se prevalente, l'opinione contraria alla possibilità di un responsabile interno è dibattuta, e senza un divieto espresso sembra che il responsabile possa essere un dipendente del titolare. Parlando della professionalità il responsabile del trattamento deve avere competenze tecniche specifiche per garantire la sicurezza dei dati, come richiesto dal Regolamento 2016/679. Secondo l'art. 28, par. 1 di questo regolamento, il responsabile deve essere scelto tra coloro che possono garantire misure tecniche e organizzative adeguate per soddisfare i requisiti normativi e proteggere i diritti degli interessati. La determinazione di quali siano le *garanzie sufficienti* sembra essere a discrezione del titolare, ma tale valutazione non può essere arbitraria, poiché la qualifica di *sufficiente* richiede anche elementi oggettivi[68].

Il responsabile è una persona, che sia fisica o giuridica, che appunto solitamente opera al di fuori dell'organizzazione del titolare ed è presa in causa per elaborare i

[68] Cfr. Farace, *Il titolare e il responsabile del trattamento* cit., pp. 755 ss.

dati personali per conto di esso: ciò che può essergli assegnato varia da un compito specifico a una mansione più generale. Il rapporto tra titolare e responsabile del trattamento è regolato dall'accordo scritto o in formato elettronico da stipularsi tra essi ai sensi dell'art. 28, par. 9, GDPR[69]: «*tale contratto deve contenere, in particolare, l'indicazione della materia disciplinata, della natura, della finalità e della durata del trattamento, del tipo di dati personali e delle categorie di interessati, delineando diritti ed obblighi del responsabile del trattamento*»[70].

La violazione di questi requisiti comporta la nullità del contratto e la responsabilità esclusiva del titolare. Il Regolamento impone anche clausole specifiche, come l'obbligo del responsabile di trattare i dati solo su istruzione documentata del titolare. Questi requisiti rappresentano un cambiamento significativo rispetto alla Direttiva 95/46, che era meno dettagliata. Il rapporto tra titolare e responsabile può essere istituito tramite vari tipi di contratti, come il mandato professionale, ma sono ammissibili anche altre forme contrattuali o clausole integrate. È possibile anche designare più responsabili del trattamento[71].

Un altro elemento rilevante che lega titolare e responsabile è dato dall'art. 30 tramite il quale si esplica l'obbligo di tenere un registro delle attività di trattamento. Questo è una sorta di diario di bordo che va aggiornato quotidianamente con tutte le attività svolte sul trattamento e, *in primis*, ogni cosa che lo riguarda. Si può dire che facilita le attività di controllo, lasciando indietro la burocrazia derivante dall'obbligo di notificazione normato dalla direttiva 95/46 e contribuendo all'impronta di *accountability* presa dal regolamento. In questo contesto, si introduce la figura del Responsabile della Protezione dei dati a cui sarà dedicato un paragrafo successivamente, per ora ci si soffermerà a dire che questa figura in combinato con il registro delle attività completa il contesto del decentramento delle forze di controllo[72].

"*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*

---

[69] Cfr. Tuccari, *I soggetti del trattamento* cit., p. 176.
[70] V. Tuccari, *I soggetti del trattamento* cit., p. *177.*
[71] Cfr. Farace, *Il titolare e il responsabile del trattamento* cit., p. 762.
[72] Cfr. Calzolaio, Ferola, Fiorillo, Rossi, Timiani, *La responsabilità e la sicurezza del trattamento* cit., pp. 147-148.

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" [73]; così recita il paragrafo 5 dell'art. 30 GDPR, per cui le imprese con meno di 250 dipendenti non sono tenute ad avere questo registro, ma con dei criteri ben precisi si spiegano i casi in cui saranno tenute allo stesso modo.

A volte, un titolare del trattamento può nominare un responsabile in modo fittizio, cioè senza rispettare le finalità previste dalla legge, ma per motivi evasivi. Ad esempio, se un'azienda vende elenchi di numeri di telefono per scopi pubblicitari senza rispettare le normative sulla privacy, l'Autorità Garante può considerare questa nomina dei terzi come responsabili del trattamento un "*artifizio illecito ed elusivo*". Secondo il principio di finalità, questa regola si applica a qualsiasi nomina strumentale che miri a eludere le norme di protezione dei dati personali[74].

Nei paragrafi 2 e 4 dell'art. 28 GDPR si stabilisce che il responsabile possa delegare dei compiti singoli e plurimi un c.d. sub-responsabile, sempre con una precedente autorizzazione scritta da parte del titolare. Quest'ultima può anche essere più generica, in questo caso il responsabile è impegnato ad aggiornare il titolare su ogni aggiunta o cambio di sub-responsabili, in modo che esso possa autorizzarle o meno. Le responsabilità che deve assumere questo soggetto sono le stesse del già precedentemente citato accordo tra titolare e responsabile, sottoscritte con un ulteriore accordo. La responsabilità delle azioni di questo soggetto rimane nelle mani del responsabile del trattamento[75].

Così come il titolare, anche il responsabile ha il potere di delegare funzioni e compiti a individui sotto la sua supervisione diretta, come stabilito dal d.lgs. n. 196/2003. Può anche fornire istruzioni a tali persone. Secondo la stessa normativa, sia il titolare che il responsabile possono stabilire le modalità per autorizzare coloro che operano sotto la loro supervisione diretta a trattare i dati personali. Il responsabile può anche trasferire dati verso Paesi esteri o organizzazioni internazionali. Il Regolamento 2016/679 specifica che il titolare può autorizzare il

[73] *GDPR consultato al link: GDPR*
[74] Cfr. Farace, *Il titolare e il responsabile del trattamento* cit., p.765.
[75] Cfr. Tuccari, *I soggetti del trattamento* cit., p. 177.

responsabile a nominare altri responsabili per condividere le responsabilità. I dettagli sui diritti, poteri e obblighi, inclusi i compensi, sono solitamente concordati nei contratti che regolano il rapporto tra titolare e responsabile[76]

Inoltre, occorre richiamare il paragrafo 2 dell'art. 33 GDPR in cui si stabilisce che il responsabile in caso di violazione dei dati personali sia obbligato a comunicarlo al titolare in modo tempestivo, così che si possano adottare le necessarie contromisure. È altrettanto rilevante il paragrafo 2 dell'art. 2 GDPR, il quale recita: "*Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento"*[77]. Come già sottolineato richiamando prima il parere n. 1 del settembre 2010 del gruppo art. 29, in questo caso si faceva solo riferimento al responsabile, nel caso in cui quest'ultimo acquistando potere decisionale sulle finalità o sui mezzi essenziali del trattamento, diventa di fatto titolare autonomo del trattamento, dovendo rispondere in termini di responsabilità civilistica nel violare il suo mandato[78].

In conclusione, tornando a parlare di *accountability*, è curioso richiamare questo caso che fa riflettere sul fatto che nel contesto giudiziario, la concreta applicazione del principio di responsabilizzazione si rivela non solo difficile da raggiungere, ma anche complessa da comprendere. Ciò emerge chiaramente dalla sentenza n. 2774/2013 emessa dal tribunale di Roma, in cui un ufficiale di un servizio guardaparco, delegato dal P.M. all'esecuzione di un decreto di sequestro probatorio, è stato ritenuto titolare del trattamento per aver affisso una copia dell'ordinanza impositiva del vincolo reale sul cancello d'ingresso di un immobile sottoposto a sequestro, includendo i dati di identificazione personale del destinatario.

---

[76] Cfr. Farace, *Il titolare e il responsabile del trattamento* cit., p. 767.
[77] *GDPR consultato al link: GDPR*
[78] Cfr. Calzolaio, Ferola, Fiorillo, Rossi, Timiani, *La responsabilità e la sicurezza del trattamento* cit., p. 153.

Il tribunale di primo grado ha interpretato l'azione dell'ufficiale di P.G. come un trattamento dei dati personali, poiché la delega dell'Autorità Giudiziaria all'esecuzione del sequestro non includeva la divulgazione dei dati. Tuttavia, poiché il P.M. non aveva specificato che il servizio Guardaparco delegato doveva trattare i dati personali dell'indagato, la divulgazione integrale dei dati è stata considerata non motivata da alcuna ragione legittima, se non quella della comodità nell'esecuzione dell'atto. Pertanto, la condotta del guardaparco è stata ritenuta lesiva del principio di minimizzazione dei dati personali, come stabilito dal GDPR.

La Corte di cassazione, chiamata a pronunciarsi sull'argomento, ha corretto le conclusioni del tribunale, sottolineando che l'ufficiale non era il responsabile dei dati personali del ricorrente, ma ha agito indebitamente come se lo fosse. La delega conferita dall'Autorità Giudiziaria per l'esecuzione del sequestro avrebbe potuto essere soddisfatta senza includere i dati personali. Così, il Guardaparco è stato ridimensionato dal ruolo di titolare del trattamento a quello di responsabile, ma la decisione della Corte suprema non ha chiarito appieno le posizioni soggettive e le relative responsabilità riguardanti il rispetto della normativa privacy nell'ambito giudiziario. La questione resta aperta sul modo in cui un ufficiale di P.G., operante su delega del pubblico ministero, possa essere considerato titolare o anche solo responsabile del trattamento dei dati[79].

1.3.2 *Il responsabile della protezione dei dati (data protection officer)*

Tra gli strumenti che più incarnano il principio di *accountability* si trova la possibilità di nominare un responsabile della protezione dei dati, sempre possibile da parte di titolari e responsabili e obbligatoria in dei casi specifici, specificamente disciplinato agli artt. 37, 38, 39. Sostanzialmente la nomina è obbligatoria: per tutti i trattamenti svolti da autorità od organismi pubblici; per tutti quei trattamenti che prevedono un monitoraggio regolare e sistematico degli interessati e su larga scala; se si prevede di trattare dati di categorie particolari o relativi a condanne penali e a reati[80].

[79] Cfr. F. Brizzi, *il GDPR in ambito giudiziario: fino a che punto può spingersi l'accountability?* in Ius Penale Gfl, 11.12.2018, consultato il 22.04.2024.
[80] Cfr. Tuccari, *I soggetti del trattamento* cit., pp. 184-185.

Pensando ai criteri che possano definire i concetti di "*larga scala*" e "*monitoraggio regolare e sistematico*" sono subito sorte delle criticità, alle quali il Gruppo di lavoro art. 29 ha fornito criteri più definiti tramite le *Linee guida sui responsabili della protezione dati* (WP 243 del 13 dicembre 2016)[81]. Citando direttamente questo documento possiamo dire che per definire su "*larga scala*" sono stati elencati i seguenti criteri: "*il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; la durata, ovvero la persistenza, dell'attività di trattamento; la portata geografica dell'attività di trattamento"*. Per quanto riguarda l'espressione "*monitoraggio regolare e sistematico*" si premette che non si intende il solo monitoraggio *online*, che viene definito dal considerando 24 elencando successivamente i significati di "*regolare*": "*che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito; ricorrente o ripetuto a intervalli costanti; che avviene in modo costante o a intervalli periodici*". Mentre per "*sistematico*" si elencano i seguenti significati: "*che avviene per sistema; predeterminato, organizzato o metodico; che ha luogo nell'ambito di un progetto complessivo di raccolta di dati; svolto nell'ambito di una strategia*", fatto salvo che basta che si assuma uno solo di questi significati[82].

Tornando all'art. 37 GDPR, si nota la possibilità di avere un responsabile della protezione dati per più titolari risultando omnicomprensivo, poiché si prevede per i gruppi imprenditoriali al par. 2 e per le associazioni di categoria di titolari al par. 4, e anche per gli organismi pubblici al par. 3, se si pensa ai piccoli comuni sarebbe insostenibile prevederne dei singoli. Lo stesso discorso si può declinare per le associazioni di categoria che comprendono solitamente piccole e medie imprese che possono così far riferimento a un unico DPO[83].

Titolare e responsabile del trattamento, una volta designato il responsabile, non esauriscono i loro doveri, ma devono svolgere alcuni compiti: inizialmente devono

---

[81] Cfr. Calzolaio, Ferola, Fiorillo, Rossi, Timiani, *La responsabilità e la sicurezza del trattamento* cit., p. 156.

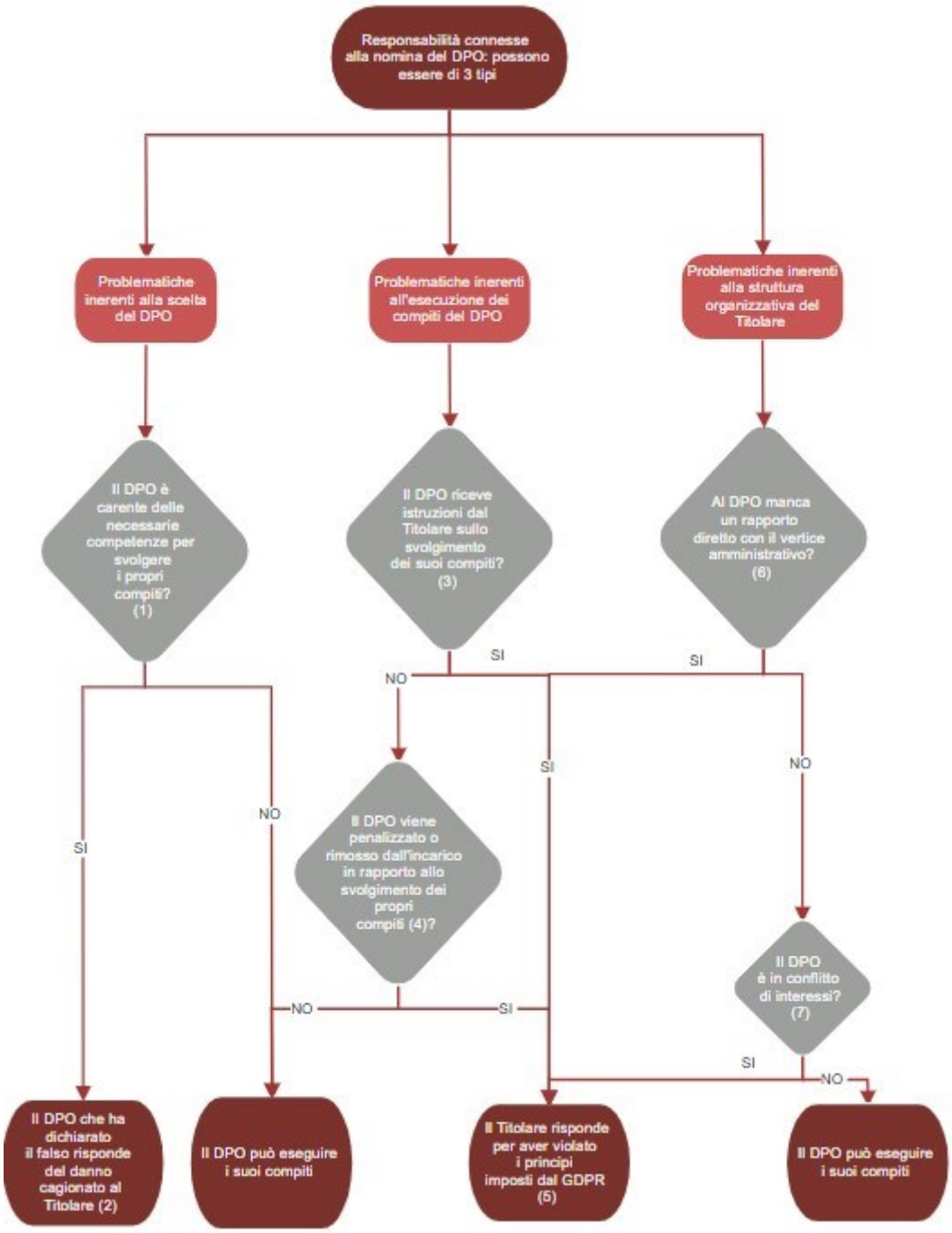
[82] Documento consultato al link: Lineee-guida-sui-responsabili-della-protezione-dei-dati-RPD-WP-243.pdf

[83] Cfr. Calzolaio, Ferola, Fiorillo, Rossi, Timiani, *La responsabilità e la sicurezza del trattamento* cit., p. 157.

assicurarsi che sia coinvolto in modo adeguato e tempestivo in tutte le attività riguardanti la protezione dei dati personali; fornire le risorse economiche e non che servono al DPO per svolgere efficacemente i propri compiti e per aggiornarsi sulle proprie competenze; assicurare l'indipendenza di questo soggetto e che quindi non riceva assolutamente nessuna istruzione per svolgere i propri compiti e alla stesso tempo riuscire a precludere ogni possibilità di che venga penalizzato o rimosso perché facendo bene il suo lavoro possa crear danno a titolare e responsabile del trattamento[84].

I compiti assegnati al responsabile della protezione dei dati sono il giusto bilanciamento tra il suo ruolo di assistenza al titolare e di sorveglianza sul rispetto del Regolamento. Dando per scontato che questo soggetto sia dotato delle qualità e conoscenze professionali adatte, come stabilito dall'art. 37 par.5, si possono individuare le funzioni di sorveglianza in primo luogo sull'operato del titolare vigilando sul rispetto del Regolamento e della valutazione di impatto che ha anche potere di giudicare tramite un parere (funzione di assistenza), avendo anche uno stretto rapporto con l'Autorità tramite la procedura di consultazione. Inoltre, ha la facoltà di attribuire responsabilità, formare e sensibilizzare il personale sulla protezione dei dati personali. In aggiunta di ciò, il DPO ha appunto la facoltà di consultare e di essere consultato da tutti i soggetti coinvolti oltre che dagli interessati. La condizione ovvia poiché tutto ciò sia possibile consiste nel fatto che lui deve avere accesso a tutti i dati personali detenuti dal titolare del trattamento[85].

[84] Cfr. Tuccari, *I soggetti del trattamento* cit., p. 185.
[85] Cfr. Calzolaio, Ferola, Fiorillo, Rossi, Timiani, *La responsabilità e la sicurezza del trattamento* cit., p. 160-161.



Questo schema è utile per fare una riflessione sulle possibili problematiche inerenti al ruolo del DPO, si districa in tre macro-casi di possibili problematiche. *In primis* nel caso che questo sia carente delle necessarie competenze per svolgere i suoi compiti, in questo caso il DPO avrebbe dichiarato il falso e andrebbe incontro alle problematiche relative al danno cagionato al titolare del trattamento. Del secondo caso si è già parlato precedentemente e la conseguenza è diretta al titolare. Mentre nel terzo ed ultimo, il DPO potrebbe avere problemi nel rapporto col vertice

amministrativo non essendo direttamente collegato e di conseguenza potrebbe verificarsi un conflitto d'interessi che porterebbe sempre a conseguenze dirette al titolare[86].

1.3.3 *Privacy by design e privacy by default*

Il principio di *accountability*, già precedentemente citato, è esplicato all'art. 5 par. 2 GDPR, dove si impone al titolare del trattamento di essere in grado di dimostrare che rispetta gli obblighi previsti dal Regolamento oltre che rispettarli in sé. Questo principio si traduce in diverse misure. Oltre agli strumenti rappresentati dalla normina del responsabile per la protezione dei dati e dell'istituzione di registri di attività del trattamento, l'art. 25 GDPR regola, infatti, i concetti di *privacy by design* e *privacy by default*: per cui si intendono come protezione dei dati fin dalla progettazione del trattamento e protezione dei dati per impostazione predefinita[87].

Il Regolamento europeo stabilisce chiaramente chi debba assumersi l'intera responsabilità della gestione dei dati personali, delineando un ruolo fondamentale per il titolare del trattamento. Questo soggetto diventa il protagonista principale e il fulcro dell'intera architettura giuridica europea in materia di protezione dei dati. È al titolare del trattamento che spetta il delicato compito di valutare e gestire i rischi associati al trattamento dei dati, e quindi anche le misure di privacy by design e by default. Questo compito non si esaurisce nella fase iniziale, ma si estende per l'intera durata del trattamento[88] .

La *privacy by design* prevede che si debba fabbricare un trattamento in modo che si attuino i principi di protezione dei dati come la minimizzazione, soddisfacendo i requisiti che impone il Regolamento; in questo caso, le modalità sono a discrezione del titolare. La *privacy by default* consiste nell'obbligo del titolare di adottare misure che permettano di trattare solo i dati necessari per le finalità del trattamento, come primo passo per la successiva progettazione, appunto di *default*. Nella pratica, la sua traduzione è nel limitare allo stretto necessario la quantità di dati raccolti, la portata

[86] Cfr. P. Spera , *Inadempimento del DPO* in Ius responsabilità civile Gfl, 18.10.2021, consultato il 19.04.2024.
[87] Cfr. Tuccari, *I soggetti del trattamento* cit., p. 180.
[88] Cfr. S. Calzolaio, *Privacy by design. Principi, dinamiche e ambizioni del nuovo Reg. UE 2016/679*, in federalismi.it, 20.12.2017, consultato il 19.04.2024.

del trattamento, il periodo di conservazione e l'accessibilità. Anche in questo caso viene detto cosa bisogna proteggere e viene lasciata libertà nel modo in cui farlo[89].

Inizialmente, si specifica che le richieste rivolte al Titolare devono essere ragionevoli e proporzionate. Questo significa che nel valutare le misure tecniche e organizzative necessarie, si tiene conto dello stato attuale della tecnologia e dei costi associati alla loro implementazione, in relazione alle caratteristiche specifiche del trattamento e alla valutazione dei rischi. Successivamente, vengono fornite delucidazioni riguardo alle misure tecniche e organizzative considerate adeguate per impostazione predefinita, come ad esempio la pseudonimizzazione, e sui principi che guidano l'architettura del modello europeo di protezione dei dati. Uno di questi principi è la minimizzazione dei dati, secondo il quale i dati personali devono essere adeguati, pertinenti e limitati a quanto strettamente necessario per le finalità del trattamento. Entrambi gli aspetti sono strettamente correlati alle dinamiche della società digitale: quanto più il trattamento dei dati presenta il rischio di una diffusione in ambiente digitale, tanto più diventano cruciali le esigenze strutturali di minimizzazione e pseudonimizzazione dei dati fin dalla fase di progettazione del trattamento[90], concetto per il quale si aprirà una breve parentesi.

La pseudonimizzazione consiste nel sostituire un attributo univoco di un dato con un altro altrettanto univoco ma di difficile comprensione. Questo processo può rendere più difficile l'identificazione dei dati, richiedendo anche mezzi costosi per collegarli alla persona, ma non cambia l'associazione tra dato e individuo. Al contrario, l'anonimizzazione mira a introdurre incertezza nell'associazione di un dato a un individuo specifico. In altre parole, la pseudonimizzazione non altera l'associazione univoca tra dato e persona, e il dato pseudonimo può essere facilmente riferito alla persona attraverso la sostituzione degli attributi originali. Questo non è il caso con un processo di anonimizzazione ben strutturato, dove la riferibilità del dato anonimizzato alla persona diventa altamente improbabile. Dopo un processo di pseudonimizzazione, la persona potrebbe ancora essere identificata indirettamente e

---

[89] Cfr. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: il Regolamento europeo 2016/679* cit., pp. 44-45.

[90] Cfr. S. Calzolaio, *Privacy by design. Principi, dinamiche e ambizioni del nuovo Reg. UE 2016/679*, in federalismi.it, 20.12.2017, consultato il 19.04.2024.

quindi la pseudonimizzazione, se ben eseguita, rappresenta solo una misura di sicurezza utile per ridurre la comprensibilità di un insieme di dati relativi a una persona[91] .

1.3.4 *Codici di condotta e meccanismi di certificazione*

Tramite l'art. 40 par. 1 GDPR si invita a elaborare codici di condotta che servano ad aiutare le aziende nella corretta applicazione del Regolamento. È previsto un meccanismo rigoroso per l'elaborazione, la modifica o proroga di questi codici. Innanzitutto, devono essere approvati dall'autorità di controllo competente. Se viene approvato, l'autorità dovrà renderlo pubblico esplicando i criteri secondo i quali è stato approvato, mentre nel caso in cui il codice si riferisca a più stati membri sarà compito del comitato europeo per la protezione dei dati formulare un parere sulla conformità del codice. Ulteriormente la Commissione potrebbe dare al codice validità generale su tutto il territorio UE[92].

Il Regolamento europeo riserva specificamente agli organismi di autoregolamentazione gli articoli 40 e 41, che insieme alle disposizioni successive sugli organismi certificatori (articoli 42 e 43) costituiscono la Sezione V del Capo IV, focalizzata sugli obblighi del titolare e del responsabile del trattamento dei dati personali. Queste disposizioni confermano l'importanza del modello di autoregolamentazione nel nuovo sistema di protezione dei dati, riformulando in parte il ruolo dei codici rispetto alla direttiva del 1995, delineando più chiaramente il loro processo di sviluppo e i controlli applicativi. In particolare, l'articolo 40 sottolinea l'autonomia dei titolari o dei responsabili del trattamento nel definire regole deontologiche, consentendo loro di elaborare codici di comportamento tramite associazioni di categoria o organismi rappresentativi. Questo è mirato a integrare i principi generali della normativa e adattarli alle specificità dei vari contesti di trattamento, inclusi i casi speciali come le imprese di piccole o medie dimensioni.

[91] Cfr. G. D'acquisto, M. Naldi, *Big data e privacy by design. Anonimizzazione Pseudonimizzazione Sicurezza*, I ed., Torino, 2017.
[92] Cfr. Tuccari, *I soggetti del trattamento* cit., p. 188.

Anche se la redazione dei codici non è obbligatoria, le autorità di controllo incentivano tale iniziativa, promuovendo così la sicurezza dei dati.

Per quanto riguarda il contenuto dei codici, l'articolo 40 elenca diverse materie che possono essere disciplinate, tra cui requisiti di correttezza e trasparenza del trattamento, raccolta dei dati personali, pseudonimizzazione dei dati, obblighi di informazione, consenso specifico per la tutela dei minori e misure di sicurezza del trattamento e dei sistemi. Questo elenco non è esaustivo ma si basa sulle disposizioni normative, fungendo da complemento e attuazione delle stesse. L'approvazione dei codici avviene attraverso un processo che coinvolge le autorità di controllo, le quali valutano la loro conformità e adeguatezza. Una volta approvati, i codici diventano efficaci e sono soggetti a monitoraggio continuo per garantirne il rispetto. Tale regime di autorizzazione assicura la conformità dei codici alla normativa europea e facilita la loro adozione anche al di fuori dell'Unione Europea, consentendo così la diffusione dei principi europei di protezione dei dati a livello globale. In sintesi, l'adozione dei codici di condotta riflette l'intento del legislatore europeo di fornire un quadro normativo flessibile e partecipativo, integrando e completando le disposizioni regolamentari con meccanismi di autoregolamentazione finalizzati a garantire un adeguato livello di protezione dei dati personali[93].

Un'altra modalità tramite cui i soggetti del trattamento possono far valere il principio di *accountability* sono i meccanismi di certificazione. Queste certificazioni sono rilasciate da organismi accreditati che possono essere l'autorità di controllo competente o un organismo designato dallo stato membro per rilasciarle. Titolare e responsabile possono decidere volontariamente se accedere a questi meccanismi o meno, traendone vantaggio in termini di reputazione. Queste certificazione durano tre anni e sono rinnovabili, ovviamente in caso di irregolarità possono essere rimosse tempestivamente dagli organi di certificazione o dall'autorità competente[94].

Nel quadro normativo europeo, la certificazione assume un ruolo cruciale come attestazione rilasciata da un ente competente e indipendente a un'azienda che dimostra di rispettare criteri volti a garantire la qualità dei suoi prodotti e servizi,

[93] Cfr. R. D'Orazio, *Art. 40-Codici di condotta* in A. Barba, S. Pagliantini (a cura di), *Commentario del diritto civile, modulo delle persone*, volume II, Milano, 2019.
[94] Cfr. Tuccari, *I soggetti del trattamento* cit., p. 189.

nonché la trasparenza e la competitività sul mercato. Questo marchio di qualità rappresenta uno strumento fondamentale per costruire la fiducia dei consumatori e promuovere una concorrenza equa. L'introduzione della protezione dei dati nel contesto della certificazione è giustificata dall'adozione di un approccio basato sulla responsabilizzazione anziché sul mero adempimento formale. Tale approccio è sostenuto dall'idea che le imprese sono incentivante a conformarsi ai principi e alle regole della protezione dei dati non solo per rispettare la normativa, ma anche per presentarsi come titolari affidabili e trasparenti agli occhi dei consumatori. Per quanto riguarda l'attuazione pratica del sistema di certificazione, la normativa europea, in particolare gli articoli 42 e 43, assegna agli Stati membri un ampio margine di discrezionalità per definire il modello più adatto. Gli articoli 42, paragrafo 5, e 58, paragrafo 3, lettera f, stabiliscono che i criteri per il rilascio della certificazione sono stabiliti dall'Autorità competente o dal Comitato. Allo stesso modo, gli articoli 43, paragrafo 1, lettera b, e 57, paragrafo 1, lettera p, definiscono che i criteri per l'accreditamento degli organismi di certificazione sono adottati dall'Autorità di garanzia o dal Comitato, in aggiunta ai criteri base stabiliti dal Regolamento. Tuttavia, l'attuazione pratica della certificazione può presentare sfide, specialmente riguardo alla definizione dei ruoli dei diversi soggetti coinvolti, come previsto dagli articoli 42, paragrafo 4, e 43, paragrafo 1. La discrezionalità concessa agli Stati membri può portare a una diversità di approcci a livello europeo anziché a un'armonizzazione desiderata[95].

[95] Cfr. Calzolaio, Ferola, Fiorillo, Rossi, Timiani, *La responsabilità e la sicurezza del trattamento* cit., pp. 165 ss.

Capitolo 2
EVOLUZIONE TECNOLOGICA: INTELLIGENZA ARTIFICIALE E UTILIZZI UTILI PER QUESTA RICERCA

2.1 **Premessa. Intelligenza artificiale: storia e principali utilizzi**

Il problema con la definizione di intelligenza artificiale è che molti pensano di capirla grazie alla letteratura e alla fantascienza, che ne hanno parlato in modo problematico per molti anni, suggerendo l'idea di macchine capaci di agire e pensare come esseri umani. Come avvenuto per la robotica, anche l'intelligenza artificiale e le sue implicazioni sociali ed etiche sono state largamente previste dalla fantascienza. Oggi, alcune delle capacità attribuite ai robot e all'intelligenza artificiale sono rese possibili dalla tecnologia e dalla scienza. La rivoluzione industriale attuale riguarda proprio l'integrazione delle macchine intelligenti nella società. Di conseguenza, ci troviamo a dover sviluppare chiavi interpretative che regolino l'inserimento delle macchine nella nostra vita, stabilendo i contesti normativi, etici e giuridici di riferimento[96].

Quando si parla di intelligenza artificiale, è cruciale comprendere che non si tratta solamente di *robot* antropomorfi che camminano e parlano come noi. Sebbene questa rappresentazione possa catturare l'immaginazione, l'IA si manifesta principalmente attraverso *software* e algoritmi. È importante notare che l'intelligenza, sia umana che artificiale, è un concetto sfuggente e complesso. Mentre gli esseri umani continuano a studiarne le sfumature, l'intelligenza artificiale si basa sulla riproduzione delle capacità umane, ma in un modo diverso: i sistemi di IA apprendono tramite il

[96] Cfr. M. C. Carrozza, C. Oddo, S. Orvieto, A. di Minin, G. Montemagni, *AI: profili tecnologici Automazione e Autonomia: dalla definizione alle possibili applicazioni dell'Intelligenza Artificiale* in BioLaw-Rivista di Biodiritto, n, 3/2019, p. 244.

riconoscimento di modelli nei dati piuttosto che attraverso il ragionamento deduttivo che è tipico della mente umana.

Negli ultimi anni, l'IA ha compiuto passi da gigante, e ciò è stato possibile grazie a due fattori principali. Da un lato, c'è stato un notevole aumento delle capacità di calcolo, consentendo ai *computer* di elaborare dati sempre più velocemente e con una memoria straordinariamente ampia. Dall'altro lato, c'è stata un'esplosione di dati digitali, grazie anche al diffondersi di sensori ad alta definizione e a basso costo. La nostra interazione quotidiana con la tecnologia digitale, che comprende la digitalizzazione di documenti, la condivisione di foto e video e l'uso di piattaforme di *social media*, contribuisce costantemente alla raccolta di dati.

Questi due fattori, insieme ad altri progressi nella ricerca, hanno reso possibile lo sviluppo e la diffusione su vasta scala dei sistemi di *machine learning*. In breve, questi sistemi consentono all'IA di apprendere autonomamente dall'ambiente circostante, modificando le proprie prestazioni in base all'esperienza accumulata. In altre parole, il *software* di IA si adatta nel tempo per raggiungere gli obiettivi stabiliti, imparando dai dati che elabora e immagazzina[97].

Per cui, prima di addentrarsi nella situazione attuale dell'IA e della tecnologia stessa che ci pervade, è doveroso ripercorrere le tappe storiche di questa evoluzione.

2.1.1 *Da Alan Turing al mondo contemporaneo*

Fin dai primordi, l'Intelligenza Artificiale ha suscitato un interrogativo cruciale: cosa rende un sistema artificiale degno di essere definito intelligente? Come hanno osservato numerosi studiosi, il dilemma dell'IA risiede nel suo stesso nome. Da una parte, comprendiamo abbastanza chiaramente il significato di "*artificiale*" (cioè qualcosa creato dall'uomo), ma dall'altra ci manca una definizione precisa di "*intelligenza*". Questo perché l'intelligenza umana è così multiforme e complessa che risulta estremamente difficile sintetizzarla in una singola definizione[98].

Fu soltanto a partire dagli anni '40 che l'idea di dare forma a un'entità *pensante* iniziò a prendere una connotazione più tangibile e realizzabile. L'avvento dei primi

[97] Cfr. G. Balbi (a cura di), *Diritto penale e intelligenza artificiale: nuovi scenari*, I ed., Torino, 2022, p. 3-4.

[98] Cfr. L. Portinale, *Intelligenza artificiale: storia, progressi e sviluppi tra speranze e timori* in MediaLaws, 28.02.2022, consultato il 4.05.2024, p. 16.

elaboratori elettronici catalizzò l'attenzione di studiosi provenienti da svariate discipline, quali psicologia, matematica, ingegneria, economia e scienze politiche, sull'effettiva fattibilità di creare un cervello artificiale. Le ricerche pionieristiche sulle macchine dotate di capacità cognitive, sviluppate in quel periodo, furono il risultato della fusione di concetti provenienti da campi scientifici diversificati. I progressi della neurologia, evidenziando la struttura neuronale del cervello e il suo funzionamento attraverso impulsi elettrochimici, si intrecciarono con le teorie cibernetiche riguardanti il controllo e la stabilità delle reti elettriche di Norbert Wiener, la teoria dell'informazione di Claude Shannon e la teoria del calcolo di Alan Turing. Questa convergenza di conoscenze naturalmente portò a interrogarsi sulla possibilità di sviluppare un cervello elettronico. In seguito, furono progettate le prime macchine basate su modelli di neuroni artificiali, tra cui *SNARC*, costruita nel 1951 da Marvin Minsky e Dean Edmonds.[99]

Il libro *Cybernetics* di Norbert Wiener ha rappresentato un punto di svolta nel mondo della tecnologia e della scienza. Pubblicato in due edizioni, la prima nel 1948 e la seconda nel 1961, questo testo ha portato idee rivoluzionarie che inizialmente sembravano strane e sorprendenti, ma che col passare del tempo sono diventate sempre più familiari e diffuse. *Cybernetics* ha segnato il passaggio da un modello di spiegazione basato sull'energia, come nella meccanica newtoniana, a uno centrato sull'informazione. Concetti come codificazione, memoria e disturbo hanno fornito una spiegazione più accurata per una vasta gamma di fenomeni, dai circuiti elettronici alle cellule biologiche.

Ciò è stato possibile perché il modello della teoria dell'informazione ha consentito di affrontare i sistemi aperti, in cui l'energia non è il problema centrale, ma piuttosto la comunicazione e il controllo con il mondo esterno. Questo cambio di paradigma ha reso obsoleti i concetti della meccanica newtoniana, mettendo in difficoltà la psicologia tradizionale ancorata a quei principi.

[99] Cfr. G.F. Italiano, *Intelligenza artificiale: passato, presente, futuro* in F. Pizzetti, *Intelligenza artificiale, protezione dei dati personali e regolazione,* I ed., Torino, 2018, p. 207.

Norbert Wiener, insieme al fisiologo Arturo Rosenblueth, sognava di creare un istituto interdisciplinare di scienziati indipendenti, desiderosi di comprendere e risolvere problemi complessi attraverso una prospettiva unificata.

Il loro lavoro ha portato alla teoria della cibernetica, un campo che studia i sistemi di comunicazione e controllo, sia meccanici che biologici. Wiener e Rosenblueth hanno trovato analogie tra dispositivi elettronici e organismi biologici, aprendo la strada a una nuova scienza che avrebbe influenzato molte discipline.

Il suo lavoro ha ispirato altri ricercatori, come Warren McCulloch e Walter Pitts, che hanno contribuito alla nascita della teoria dell'informazione e dei calcolatori digitali. Tuttavia, l'approccio della *cibernetica* alla modellizzazione dei sistemi biologici si è rivelato limitato, mentre il livello informatico, basato sulla manipolazione dei simboli, ha portato a risultati più significativi nel campo della psicologia dei processi cognitivi. Il lavoro di Norbert Wiener e dei suoi contemporanei ha aperto nuove prospettive nel mondo della scienza e della tecnologia, influenzando il modo in cui comprendiamo e interagiamo con il mondo che ci circonda[100].

Alan Turing è una figura centrale nella storia dell'informatica e dell'intelligenza artificiale. Il suo contributo più notevole è la *macchina di Turing*, un'astrazione teorica che ha dimostrato la possibilità di eseguire qualsiasi algoritmo con un dispositivo che esegue operazioni elementari su un nastro infinito. Questa idea ha gettato le basi per il concetto di calcolatore digitale moderno. Durante la Seconda Guerra Mondiale, Turing lavorò al progetto *Ultra* a Bletchley Park, dove fu coinvolto nello sforzo per decifrare i messaggi cifrati tedeschi. Qui contribuì in modo significativo alla progettazione e all'utilizzo di un calcolatore che utilizzava il concetto di macchina di Turing per analizzare e decodificare i messaggi, svolgendo un ruolo cruciale nella vittoria degli Alleati.

Inoltre, Turing ha avuto un impatto duraturo nel campo della logica matematica, dimostrando che certi problemi non possono essere risolti mediante alcun procedimento definito. Questo ha portato alla definizione di ciò che è ora noto come

[100] Cfr. P. McCorduck, *Storia dell'intelligenza artificiale: gli uomini, le idee, le prospettive,* I ed., Trento, 1987, pp. 55-60.

problema della decisione, che ha importanti implicazioni nella teoria dell'informatica e dell'intelligenza artificiale[101].

Nel 1942, Turing compì un rischioso viaggio attraverso l'Atlantico fino agli Stati Uniti, dove rimase dal novembre al marzo dell'anno successivo. Qui si dice abbia parlato con John von Neumann, anche se non c'è prova diretta che abbia appreso di altri lavori simili al suo. Tuttavia, sembra che il loro incontro abbia stimolato entrambi, con un fruttuoso scambio di idee. Dopo la guerra, Turing si unì al *National Physical Laboratory* di Teddington, iniziando a lavorare alla progettazione dell'*ACE* (*Automatic Computing Engine*), un omaggio alla *Macchina Analitica* di Babbage. Mentre si dedicava al progetto *ACE*, Turing iniziò a elaborare idee audaci riguardanti le macchine intelligenti. Nel suo saggio *Intelligent Machinery*, discuteva dei possibili modi in cui le macchine potrebbero dimostrare un comportamento intelligente, prendendo spunto dall'analogia con il cervello umano. Proseguì esaminando le potenzialità e le sfide legate alla realizzazione di macchine pensanti, suggerendo modelli e concetti di apprendimento. La sua visione audace includeva la costruzione di un *cervello artificiale* capace di compiere compiti complessi come il gioco degli scacchi, la traduzione linguistica e la crittografia. Turing pose le basi per la futura ricerca nell'ambito dell'intelligenza artificiale, anticipando molti dei concetti e degli sviluppi che avrebbero caratterizzato questo campo nei decenni successivi. La sua visione e il suo lavoro hanno influenzato in modo significativo la nostra comprensione delle potenzialità e dei limiti delle macchine intelligenti[102].

Turing può essere considerato il padre dell'IA in senso pratico, visto che si inizia a parlare di questa grazie all'avvento dei calcolatori elettronici derivanti dalle sue teorie. Durante l'estate del 1956, un gruppo di accademici si riunisce presso il Dartmouth College con l'intento di esplorare l'idea che ogni aspetto dell'apprendimento o qualsiasi caratteristica dell'intelligenza possa essere descritto in modo così preciso da consentire a una macchina di simulare tali processi. Questo incontro segna l'inizio formale di una nuova disciplina, proposta dal matematico John McCarthy, all'epoca assistente professore a Dartmouth e uno dei promotori del

[101] Cfr. Mcorduck, *Storia dell'intelligenza artificiale: gli uomini, le idee, le prospettive* cit, pp. 61-67.
[102] Cfr. MCorduck, *Storia dell'intelligenza artificiale: gli uomini, le idee, le prospettive* cit. p. 67-77.

seminario, con il nome di *intelligenza artificiale*, per questo motivo è lui ad essere considerato il "padre" dell'IA. Gli altri promotori includono Marvin Minsky, ricercatore di matematica e neurologia ad Harvard, Nathaniel Rochester, direttore della ricerca sull'informazione presso un centro di ricerca *IBM*, e Claude Shannon, il già citato matematico rinomato per la sua teoria dell'informazione, allora impiegato presso i *Bell Telephone Laboratories*. Il seminario aveva il formato di un *brainstorming*, un dibattito aperto e poco strutturato, che ha portato a un nuovo approccio teorico attraverso discussioni collettive. Tale approccio era volto a esplorare la possibilità di replicare parzialmente l'intelligenza attraverso un elaboratore elettronico. L'obiettivo del seminario era di esaminare e analizzare i programmi che dimostravano prestazioni considerate intelligenti, come il *Logic Theorist* (*LT*) di Newell, Shaw e Simon, capace di dimostrare teoremi di logica del primo ordine, e di delineare una serie di obiettivi ambiziosi da raggiungere entro dieci anni, al prossimo incontro[103].

Nei primi anni dell'intelligenza artificiale, c'era ciò che John McCarthy definisce il periodo del "*guidare la bici senza mani*", caratterizzato da un grande ottimismo e da aspettative molto alte sulle capacità dell'IA. Figure di spicco come Herbert Simon (Premio Nobel per l'economia nel 1978 e Premio Turing nel 1975) e Marvin Minsky (Premio Turing nel 1969) arrivarono addirittura a fare previsioni audaci:

- "Entro trent'anni, le macchine saranno in grado di svolgere qualsiasi lavoro umano" (H. Simon, 1965).

- "Nel giro di una generazione, il problema della creazione di un'intelligenza artificiale sarà sostanzialmente risolto" (M. Minsky, 1967).

- "Tra tre e otto anni, avremo una macchina con l'intelligenza generale di un essere umano medio" (M. Minsky, 1970).

Tuttavia, nessuna di queste previsioni si avverò, poiché i problemi legati al rendere l'IA un successo si rivelarono molto più complessi di quanto inizialmente previsto[104].

---

[103] Cfr. M. Sovalmico, *Intelligenza artificiale* in *Progetto di Intelligenza artificiale e robotica,* Politecnico di Milano, 1987, p. 4.

[104] Cfr. L. Portinale, *Intelligenza artificiale: storia, progressi e sviluppi tra speranze e timori* in MediaLaws, 28.02.2022, consultato il 4.05.2024, p. 17-18.

Dopo il workshop di Dartmouth, gli anni successivi furono caratterizzati da un significativo progresso e successi per l'Intelligenza Artificiale. Indicativamente, è possibile distinguere due tendenze principali: da un lato, il gruppo guidato da Newell, Shaw e Simon, interessato a simulare i processi cognitivi umani attraverso l'uso dei computer. Con il loro *GPS* (*General Problem Solver*) del 1958, miravano a estendere l'applicabilità del programma oltre le mere applicazioni logiche (paradigma della simulazione). Dall'altro lato, vi erano coloro che concentravano i loro sforzi sul raggiungimento delle migliori prestazioni possibili per i programmi, indipendentemente dal fatto che seguissero procedure più o meno simili ai processi umani (paradigma della prestazione o dell'emulazione). In questo periodo, si assiste a un temporaneo declino dei modelli a reti neurali, che sarebbero rinati circa trent'anni dopo, in seguito alla critica di Minsky al Perceptron di Frank Rosenblatt, il quale non era in grado di riconoscere stimoli visivi anche molto semplici[105].

Grazie a nuove metodologie e tecniche innovative, i computer di quel periodo riuscirono a risolvere problemi algebrici complessi, dimostrare teoremi geometrici e persino comunicare in inglese con un buon livello di competenza. Questi risultati sorprendenti erano difficilmente immaginabili solo pochi anni prima. Tra il 1956 e il 1974, l'Intelligenza Artificiale viveva il suo periodo d'oro, supportata anche da finanziamenti consistenti da parte di agenzie governative come la *Defense Advanced Research Projects Agency* (*DARPA*). In quegli anni, si cominciò a studiare il ragionamento umano come un processo di ricerca in uno spazio adatto, con molti algoritmi dell'IA basati su questo concetto. Per raggiungere un obiettivo specifico, come vincere un gioco o dimostrare un teorema, si progettavano algoritmi che esploravano passo dopo passo uno spazio di ricerca. Tuttavia, questo approccio poteva essere limitato dalla vastità dello spazio delle soluzioni, noto come *esplosione combinatoria*, soprattutto in casi come il gioco degli scacchi. Per affrontare questo problema, i ricercatori svilupparono euristiche per ridurre il numero di opzioni da esplorare, ottenendo risultati impressionanti come la risoluzione di problemi geometrici e algebrici non banali, e il controllo dei primi *robot*[106].

---

[105] Cfr. Sovalmico, *Intelligenza artificiale* in *Progetto di Intelligenza artificiale e robotica* cit., p. 5.
[106] Cfr. Italiano, *Intelligenza artificiale: passato, presente, futuro* cit., pp. 209-210.

Dopo questo primo periodo d'oro si può dire che l'Intelligenza Artificiale ha attraversato un ciclo di *stagioni*, alternando periodi di delusione e fallimento a periodi di entusiasmo e successo. Il primo *inverno* dell'IA ha avuto inizio negli anni '70, più precisamente tra il 1974 e il 1980, quando divenne evidente che sviluppare sistemi capaci di sfruttare la conoscenza umana era estremamente difficile. Inoltre, i limiti degli approcci basati sulla logica formale, che dominavano all'epoca, divennero chiari, soprattutto nelle situazioni che richiedevano l'uso di conoscenze incerte e il ragionamento in condizioni di incertezza. In aggiunta, una scoperta nota come il *paradosso di Moravec* ebbe un impatto significativo nell'ambito dell'IA. Contrariamente alle supposizioni tradizionali, si rivelò che l'elaborazione sensoriale di base e la percezione richiedevano notevolmente più risorse computazionali rispetto ai processi di ragionamento ad alto livello. In altre parole, risultò più facile costruire un sistema in grado di giocare a giochi intelligenti come gli scacchi a un livello comparabile a quello di un campione umano, piuttosto che sviluppare un sistema con le stesse capacità sensoriali di un bambino di due anni[107].

È doveroso esplorare nello specifico i motivi che portarono a ciò; oltre a questo paradosso, l'Intelligenza Artificiale si trovava, infatti, di fronte a numerose sfide. Innanzitutto, le tecnologie disponibili all'epoca non erano in grado di fornire il potere computazionale necessario per molte applicazioni dell'IA, come l'elaborazione del linguaggio naturale o la visione artificiale. Anche i *supercomputer* più avanzati avevano solo una frazione della potenza di calcolo richiesta. Inoltre, emerse che molti problemi erano estremamente difficili da risolvere in modo efficiente, richiedendo risorse di calcolo considerevoli. Questa sfida era evidenziata dai lavori pionieristici di Cook e Karp sulla teoria della *NP-completezza*. Inoltre, la gestione dei dati costituiva un'altra grande difficoltà: molte applicazioni richiedevano enormi quantità di informazioni, ma non c'era la capacità di costruire o gestire basi di dati così estese, né di far apprendere queste informazioni alle applicazioni software[108].

Questa *dose di realtà* ha portato, in quegli anni, a una maggiore focalizzazione su ambiti di competenza più ristretti, con la creazione dei primi sistemi esperti. In questi

[107] Cfr. Portinale, *Intelligenza artificiale: storia, progressi e sviluppi tra speranze e timori* cit., p.18.
[108] Cfr. Italiano, *Intelligenza artificiale: passato, presente, futuro* cit., p. 213.

sistemi, una conoscenza dettagliata e approfondita dello specifico settore di applicazione è fondamentale. Non si tratta più solo di comprensione teorica del problema, ma anche di regole pratiche derivate dall'esperienza. In un sistema esperto, queste due forme di conoscenza, tipiche di un esperto umano in un determinato campo, vengono codificate e rappresentate in modo che il computer possa utilizzarle per risolvere problemi simili a quelli affrontati dall'esperto umano. Il primo sistema esperto, *DENDRAL*, è stato sviluppato per dedurre la struttura delle molecole organiche dalle loro formule chimiche; *MYCIN*, forse il sistema esperto più noto, utilizza conoscenze mediche specifiche per diagnosticare e prescrivere trattamenti per infezioni batteriche del sangue, anche in presenza di informazioni incomplete o incerte. L'importanza della conoscenza del settore è evidente anche nella comprensione del linguaggio naturale: in questi anni si osserva un passaggio dall'attenzione alla sintassi a quella per la semantica, ottenendo risultati interessanti[109].

Le stesse agenzie che fino a quel momento avevano finanziato generosamente la ricerca in Intelligenza Artificiale, come *DARPA*, il *National Research Council* (*NRC*) e il governo del Regno Unito, iniziarono a manifestare frustrazione per la mancanza di progressi nell'area e alla fine decisero di ridurre drasticamente i finanziamenti. Questo *trend* ebbe inizio già nella seconda metà degli anni '60 negli Stati Uniti, quando un rapporto dell'*Automatic Language Processing Advisory Committee* (*ALPAC*) criticò duramente l'efficacia degli sforzi dei ricercatori nell'elaborazione del linguaggio naturale. Dopo aver investito oltre 20 milioni di dollari nei suoi programmi di ricerca, il *National Research Council* interruppe prematuramente i finanziamenti. Negli stessi anni, nel Regno Unito, James Lighthill effettuò una valutazione della ricerca accademica nel campo dell'Intelligenza Artificiale per conto del *British Science Research Council*. Il rapporto, pubblicato nel 1973, fornì una valutazione molto pessimistica dello stato della ricerca in Intelligenza Artificiale, affermando che "*in nessun ambito del settore le scoperte fatte fino a quel momento hanno prodotto l'impatto significativo che era stato promesso*". Il *rapporto Lighthill*

[109] Cfr. Sovalmico, *Intelligenza artificiale* in *Progetto di Intelligenza artificiale e robotica*, cit., p. 5.

sottolineava esplicitamente che i ricercatori di Intelligenza Artificiale avevano fallito nel risolvere l'*esplosione combinatoria* che si presentava nelle applicazioni reali[110].

Il precedentemente citato passaggio ai sistemi esperti anche detti *weak AI* risultò una buona scelta, poiché ci si concentrò sul lato che in quel momento poteva davvero funzionare. In merito a ciò va fatta una piccola digressione su come l'IA si divida in IA forte (*strong* AI) e IA debole (*weak AI)*. Secondo la *strong AI*, il *computer* non è solo uno strumento per studiare la mente, ma, come afferma John Searle, un *computer* programmato nel modo giusto può comprendere e avere certi stati cognitivi. Per dimostrare che però non può raggiungere il livello cognitivo della mente umana, Searle propose l'esperimento della *Stanza Cinese*. Bisogna immaginarsi un programma che, seguendo complesse regole, produce risposte in cinese a partire da *input* in cinese. Anche se il programma supera il test di Turing, Searle sostiene che non comprende realmente ciò che fa. Egli immagina sé stesso seguendo istruzioni in inglese per manipolare caratteri cinesi: potrebbe sembrare che capisca il cinese, ma in realtà non lo comprende, dimostrando che lo stesso vale per il programma. La *strong AI* non ha ricevuto molta attenzione nell'informatica, dove ci si è concentrati sugli aspetti pratici di costruire sistemi che mostrino comportamenti intelligenti. La *weak AI*, invece, si prefigge di sviluppare *software* che esibiscano intelligenza in compiti specifici e limitati. Un programma che diagnostica una malattia in un campo medico specifico è considerato intelligente secondo la *weak AI*, anche se non comprende linguaggi naturali, non riconosce oggetti fisici e non gioca a tris[111].

All'inizio degli anni '80, l'Intelligenza Artificiale visse una rinascita con l'avvento di questi sistemi esperti, capaci di risolvere problemi specifici utilizzando regole basate sull'esperienza e la conoscenza degli esperti. Nel 1980, Carnegie-Mellon sviluppò *XCON* per la *Digital Equipment Corporation*, risparmiando circa 40 milioni di dollari all'anno. Questo successo spinse molte industrie a investire massicciamente e, nel 1985, gli investimenti ammontavano a miliardi di dollari. Nacquero aziende come *Symbolics*, specializzate in *hardware* per sistemi esperti. Questi sistemi

[110] Cfr. Italiano, *Intelligenza artificiale: passato, presente, futuro*, cit., p. 214.
[111] Cfr. Portinale, *Intelligenza artificiale: storia, progressi e sviluppi tra speranze e timori* cit., p. 17.

basavano la loro potenza sulla rappresentazione e l'utilizzo della conoscenza, riconoscendo che il comportamento intelligente richiede l'uso pratico di molte informazioni. La ricerca si concentrò sui sistemi basati sulla conoscenza e sull'ingegneria della conoscenza. Emerse anche il primo *software* capace di giocare a scacchi a livello di esperti umani. Questo rinnovato entusiasmo portò nuovi finanziamenti: nel 1981, il governo giapponese lanciò il progetto per i *computer* di quinta generazione, con 850 milioni di dollari, seguito da investimenti del Regno Unito e da *DARPA*, che triplicò i finanziamenti all'IA tra il 1984 e il 1988. Tuttavia, questi investimenti si trasformarono in una bolla[112].

Come appena detto, in Giappone iniziò il progetto dei *Computer di Quinta Generazione*, con l'obiettivo di utilizzare la programmazione logica basata su *PROLOG* per costruire sistemi di IA. *PROLOG*, un linguaggio di programmazione nato in Europa, è progettato per implementare il ragionamento basato su regole, con una semantica formale basata sulla risoluzione con le clausole di Horn. A quel tempo, il principale linguaggio per sviluppare sistemi basati sulla conoscenza era *LISP*, proposto da John McCarthy, che divenne lo standard nell'industria dei sistemi esperti, specialmente negli USA. Alcune aziende iniziarono a costruire e vendere computer specifici chiamati *Lisp Machines*, progettati per eseguire efficientemente il linguaggio *LISP* grazie a supporti hardware specifici. *LISP*, uno dei primi linguaggi funzionali influenzato dal lambda calcolo di Alonzo Church, era particolarmente adatto alla manipolazione simbolica necessaria ai sistemi di IA di quel periodo. Il progetto dei *Computer di Quinta Generazione* fu anche una risposta giapponese alle iniziative commerciali delle aziende americane. Nonostante il fallimento del progetto originale, *PROLOG* è ancora utilizzato in molti sistemi di IA, specialmente nelle sue versioni moderne, che permettono di affrontare in modo efficiente compiti di ottimizzazione combinatoria come la programmazione di orari, l'allocazione di risorse, la progettazione e la pianificazione[113].

Nel 1987, le principali aziende *hardware* specializzate entrarono in crisi quando *Apple* e *IBM* introdussero *desktop* economici e potenti quanto le *Lisp Machines*.

[112] Cfr. Italiano, *Intelligenza artificiale: passato, presente, futuro* cit., p. 215.
[113] Cfr. Portinale, *Intelligenza artificiale: storia, progressi e sviluppi tra speranze e timori* cit., p. 19.

Anche i sistemi esperti mostrarono i loro limiti: costosi, difficili da aggiornare, privi di capacità di apprendimento e poco robusti. Di conseguenza, i finanziamenti all'IA furono nuovamente tagliati. Alla fine degli anni '80, il programma di ricerca della *Strategic Computing Initiative* di *DARPA* fu bruscamente interrotto. Anche in Giappone la situazione non fu molto migliore: nel 1991, gli ambiziosi obiettivi del *Fifth Generation Project*, lanciato nel 1981, erano ancora lontani dall'essere raggiunti. Alcuni traguardi, come la capacità di conversare con un essere umano, furono ottenuti solo molti anni dopo, nel 2010. Come già avvenuto in passato, le aspettative create dai ricercatori di Intelligenza Artificiale erano troppo alte e irrealizzabili per l'epoca. Questo portò al secondo inverno dell'Intelligenza Artificiale, che durò circa dal 1987 al 1993[114].

Il principale ostacolo da risolvere era l'acquisizione della conoscenza. La chiave per il funzionamento di un sistema esperto è la *base di conoscenza*, un archivio di informazioni specifiche utilizzate dal sistema per svolgere i propri compiti. Questa conoscenza doveva essere raccolta manualmente tramite la collaborazione tra un esperto del settore e un ingegnere della conoscenza (specialista in IA, ma non nel settore specifico). Questa fase si rivelò la più difficile nello sviluppo dei sistemi esperti. La mancanza di metodi pratici di *machine learning* per acquisire automaticamente la conoscenza, unita a queste difficoltà, segnò la fine dell'era dei sistemi esperti. Anche i modelli *connessionistici*, che potevano utilizzare i dati grezzi per apprendere i parametri di sistema, si scontrarono con la complessità del mondo reale e le limitate capacità di apprendimento dell'epoca non offrivano soluzioni pratiche. Il mercato delle macchine *LISP* crollò, costringendo le aziende a tornare ad applicazioni tradizionali.

Negli anni '90, un rinnovato interesse per l'IA emerse con l'uso diffuso dei metodi probabilistici. Un punto di svolta fu il libro di Judea Pearl che proponeva l'uso del calcolo delle probabilità per la modellazione e l'inferenza nei sistemi intelligenti. Nonostante iniziali resistenze, Pearl dimostrò che la teoria probabilistica poteva essere coerentemente interpretata attraverso i *modelli grafici robabilistici*, in particolare le *reti bayesiane*. Questi modelli permettevano una rappresentazione

[114] Cfr. Italiano, *Intelligenza artificiale: passato, presente, futuro* cit., p. 215-216.

compatta ed efficiente della conoscenza incerta e l'uso di algoritmi di inferenza specializzati, superando molte limitazioni dei sistemi basati sulla logica.

All'inizio del nuovo millennio, Microsoft assunse ricercatori di punta nel campo delle *reti bayesiane* per avviare una nuova divisione di ricerca sull'IA e il *machine learning*. Questo *team* sviluppò applicazioni di successo come il primo filtro *spam* basato su *machine learning*, l'*Answer Wizard*, il *Windows Printer Troubleshooter* e la piattaforma di *machine learning* di *Microsoft*, ora *Azure*. Inoltre, rilasciarono uno dei primi strumenti grafici per le *reti bayesiane*, l'*MSB1*. L'adozione dei *modelli grafici probabilistici* da parte di varie aziende, nonostante la fine dell'era dei sistemi esperti, stimolò un rinnovato interesse per i sistemi intelligenti. Parallelamente, il *machine learning* divenne sempre più capace di affrontare problemi reali grazie a nuovi metodi statistici come le *Support Vector Machines* e gli approcci di *ensemble learning*, che migliorano le previsioni combinando più modelli o dati. Questi progressi portarono a una rinascita dell'interesse per l'IA e a un maggiore coinvolgimento di ricercatori e professionisti di diversi settori. Questa *nuova primavera* dell'IA, evolutasi circa dieci anni fa, inaugurò un'era dominata dai big data e da numerosi successi in vari ambiti[115].

2.1.2 L'Intelligenza Artificiale oggi e i suoi principali utilizzi

Nel 2010, la rivista *The Economist* pubblicò una copertina intitolata *The data deluge* (Il diluvio di dati), con un'immagine che rappresentava l'inizio dell'era dei *big data*. Questa nuova era permise all'IA di sfruttare enormi quantità di dati provenienti da dispositivi elettronici e attività umane. Tuttavia, il successo dell'IA non dipese solo dalla disponibilità dei dati, ma anche dallo sviluppo di nuovi formalismi e dall'aumento delle risorse computazionali come *CPU multi-core* e *GPU* avanzate. In questo contesto, le reti neurali si sono evolute in *deep neural networks*, dando vita al *deep learning*. Questo approccio rappresenta un sottoinsieme del *machine learning* che consente di gestire reti con molti strati di neuroni, cosa prima impensabile. Oggi, grazie a nuovi metodi per superare problemi di apprendimento come la scomparsa o

[115] Cfr. Portinale, *Intelligenza artificiale: storia, progressi e sviluppi tra speranze e timori*, cit., pp. 19-21.

l'esplosione del gradiente e alle potenti *GPU*, è possibile costruire e addestrare modelli molto profondi.

Il *deep learning* risolve anche la sfida dell'estrazione delle caratteristiche, automatizzando un processo che prima era manuale. Ad esempio, le *Convolutional Neural Networks* (*CNN*) possono estrarre automaticamente caratteristiche rilevanti dalle immagini, migliorando il riconoscimento degli oggetti senza la necessità di scomporre l'immagine. Questo concetto di *feature embedding* consente di rappresentare numericamente oggetti complessi, facilitando compiti come la classificazione e l'interpretazione di dati. Il successo del *deep learning* è evidente in molte applicazioni, anche se in alcuni casi è necessaria una spiegazione dettagliata delle decisioni prese dai modelli. Questo ha portato alla nascita della *Explainable AI* (*XAI*), che mira a fornire spiegazioni comprensibili per le risposte generate dai sistemi IA. Tuttavia, estrarre regole esplicative da una rete neurale non è semplice, e la combinazione di approcci simbolici e sub-simbolici è un'area di grande interesse. Un'altra sfida del *deep learning* è la vulnerabilità agli attacchi di *adversarial machine learning*, dove piccole modifiche ai dati di *input* possono ingannare i modelli, causando errori di classificazione. Ad esempio, una rete neurale che riconosce correttamente un panda potrebbe identificarlo erroneamente come un gibbone dopo piccole perturbazioni nei *pixel*, non percepibili dall'occhio umano. Questo problema è cruciale, soprattutto per applicazioni come veicoli autonomi, dove errori del genere possono avere conseguenze gravi. L*'adversarial machine learning* è quindi diventato un importante campo di ricerca per migliorare la robustezza e la sicurezza dei sistemi IA[116].

Uno degli sviluppi più rilevanti dell'intelligenza artificiale tra il 2016 e il 2018 è stato probabilmente l'aumento degli investimenti da parte di governi e industrie. In Italia, il governo ha stanziato 45 milioni di euro per IA e *blockchain*, mentre negli Stati Uniti nel 2016 sono stati assegnati 900 milioni di dollari per la ricerca, con ulteriori investimenti privati tra i 15 e i 23 milioni. In Cina, il Ministero delle Finanze ha pianificato di investire un miliardo di dollari all'anno fino al 2030 Aziende come

[116]Cfr. Portinale, *Intelligenza artificiale: storia, progressi e sviluppi tra speranze e timori* cit., pp. 21-23.

Alibaba hanno annunciato piani per investire 15 miliardi di dollari, mentre il *Vision Fund* di *SoftBank* sta concentrando una parte significativa dei suoi 100 miliardi di dollari sull'IA. Secondo un rapporto di Elsevier, il numero di pubblicazioni scientifiche sull'intelligenza artificiale è aumentato da 10.000 a 60.000 dal 1998 al 2017. Il rapporto evidenzia che, a livello globale, la ricerca sull'IA è cresciuta di oltre il 12% annuo tra il 2013 e il 2017, rispetto a meno del 5% nei cinque anni precedenti (2008-2012). La produzione complessiva di ricerca in tutte le aree tematiche correlate all'IA è aumentata dello 0,8% annuo negli ultimi cinque anni. Dopo Cina e Stati Uniti, l'India è diventata il terzo paese per risultati nella ricerca sull'IA, seguita da Germania e Giappone. Tuttavia, definire esattamente l'oggetto di tutti questi investimenti è complesso. Il campo dell'intelligenza artificiale ha molteplici definizioni e manca di un significato universalmente accettato. Vi sono più differenze che somiglianze nel modo in cui l'IA è discussa nei settori dell'educazione, della ricerca, dell'industria e dei media. Tanto che Elsevier, per redigere il suo rapporto sull'IA, ha utilizzato tecniche di IA per definire lo stesso campo dell'IA[117].

Le possibilità d'uso dei sistemi di intelligenza artificiale sono vastissime, ma catalogarle tutte è difficile per la loro vastità e diversità di settori interessati. La visione prevalente nello sviluppo di tali sistemi è quella dell'agire razionale, che abbraccia un concetto di intelligenza più ampio, legato non solo alle capacità intellettuali, ma anche alla capacità di interagire con il mondo circostante. Questo approccio mette sempre più l'accento sull'efficienza dei risultati piuttosto che sulla loro universalità, portando allo sviluppo di sistemi con competenze molto specifiche in contesti definiti anziché sistemi generici applicabili in diversi contesti.

Le aree di applicazione dei sistemi di intelligenza artificiale includono:

Pianificazione autonoma di attività e operazioni: Utilizzata soprattutto nell'industria e nella logistica, ma anche in applicazioni come le sonde spaziali. Questi sistemi sono in grado di ricevere obiettivi generali, creare piani dettagliati per raggiungerli e monitorare l'esecuzione del piano.

[117] Cfr. A. Santosuosso, *Intelligenza artificiale e diritto perché le tecnologie di IA sono una grande opportunità per il diritto,* Firenze, I ed., 2020, p. 5-6.

Giochi: Un campo tradizionale dell'intelligenza artificiale che ha portato allo sviluppo di molte tecniche, come la ricerca nello spazio degli stati. Nel 1997, ad esempio, Deep Blue della IBM ha sconfitto il campione del mondo di scacchi Garry Kasparov.

Controllo autonomo: Utilizzato nel controllo di sistemi complessi come automobili e sonde spaziali.

Dimostrazione automatica di teoremi matematici e programmazione automatica: Queste aree implicano la ricerca teorica e mirano a sviluppare tecniche per dedurre nuove informazioni da un insieme di fatti noti. Ciò influisce sulla progettazione di sistemi esperti e sistemi di domanda e risposta, nonché sulla produzione di software.

Robotica e visione artificiale: La robotica intelligente si concentra sulla manipolazione e navigazione, mentre la visione artificiale riguarda l'elaborazione di informazioni visive per riconoscere oggetti e scene. Queste tecnologie mirano a creare macchine autonome capaci di svolgere attività manuali e di percepire l'ambiente circostante.

Elaborazione del linguaggio naturale: Affronta la sfida di far comprendere e generare linguaggio naturale da parte delle macchine. Anche se i risultati attuali sono limitati, ci sono applicazioni come la consultazione di database e la traduzione.

Sistemi esperti e ontologie: Questi sistemi consentono di rappresentare la conoscenza e risolvere problemi senza la necessità di programmare algoritmi specifici. Le ontologie, descrizioni formali di domini specifici, promettono di aprire nuove applicazioni, soprattutto nel contesto web.

Queste sono solo alcune delle molte applicazioni dell'intelligenza artificiale, che continua a espandersi in nuovi settori come l'elaborazione dei segnali, l'analisi dei dati, l'*entertainment* e la medicina. La sua natura dinamica e ricca di prospettive promettenti la rende una disciplina in costante evoluzione[118].

In questo elaborato si procederà a descrivere quattro ambiti di applicazione dell'IA come *smart assistant* e *smart cars*, *robot* e *IA generative* e, in aggiunta, la tecnologia *cloud*, che è quella che si pone dietro a ognuno di questi ambiti e altri per

[118] Cfr. F. Amigoni, V. Schiaffonati, M. Somalvico, *Intelligenza artificiale* in Enciclopedia della scienza e della tecnica Treccani, 2008.

poter immagazzinare i dati. Si è scelto di descrivere questi ambiti di applicazone poiché, come si vedrà nel capitolo successivo, sono quelli che portano a dei profili critici in riferimento al GDPR.

2.2 **Internet of things e Big data**

Per poter navigare su internet, è necessario dare il consenso al trattamento dei dati. Ma perché questo consenso è richiesto con tanta insistenza? Principalmente per scopi di profilazione commerciale, e non solo. Una delle prime aziende a capire il valore di questo approccio è stata *Google*, uno dei motori di ricerca più popolari al mondo. Per mantenersi competitiva, *Google* ha iniziato a profilare gli utenti del suo sito in modo anonimo, permettendo all'azienda di conoscere interessi, gusti e preferenze dei navigatori. Questo ha un grande impatto economico, poiché la profilazione consente di fare pubblicità mirata e più efficace, oltre a vendere i dati a terzi che li utilizzano per le loro strategie produttive o pubblicitarie. Questo fenomeno è noto come *capitalismo della sorveglianza*, volto a estrarre il maggior numero possibile di dati, che, una volta aggregati, costituiscono un enorme valore economico. Questa pratica spiega la crescente ricchezza di società come *Google*, *Facebook*, *Instagram*, *WhatsApp*, *YouTube* e *Amazon*, che devono una buona parte del loro successo proprio all'estrazione e trattamento dei dati, tanto che i *big data* sono stati definiti il nuovo petrolio. Inoltre, non forniamo dati solo navigando in internet, ma anche usando dispositivi connessi, come *smartwatches* o altri *wearable*, che trasmettono informazioni sulla nostra localizzazione, salute, condizione fisica, attività e altro ancora. Pensiamo anche all'*Internet delle Cose* (*IoT*), dove dispositivi domestici come il riscaldamento, il televisore e il frigorifero sono connessi a internet e forniscono continuamente dati sulla nostra casa e attività. In definitiva, si tratta di una massa di dati enorme e in costante crescita, raccolti a costo quasi nullo,

aggregati, trattati, venduti e sfruttati per profilare gli utenti e conoscere le loro abitudini[119].

Alcuni anni fa, i ricercatori della School of Information di Berkeley hanno stimato che l'umanità avesse accumulato circa 12 *exabyte* di dati fino all'era dei computer, raggiungendo poi 180 *exabyte* già entro il 2006. Uno studio più recente indica che tra il 2006 e il 2011 il totale è cresciuto a oltre 1600 *exabyte*, superando così la soglia dello *zettabyte* (1000 *exabyte*). Questo numero tende a quadruplicare ogni tre anni, avendo portato a 8 *zettabyte* di dati nel 2015. Ogni giorno viene generata una quantità di dati sufficiente a riempire più di otto volte tutte le biblioteche americane. Naturalmente, una moltitudine di dispositivi *ICT* è costantemente impegnata per aiutarci a navigare in questo mare di dati. Questi numeri continueranno a crescere rapidamente e ininterrottamente nel prossimo futuro, soprattutto perché tali dispositivi sono tra le principali fonti di nuovi dati, che a loro volta richiedono o rendono possibili nuove tecnologie *ICT*. È un ciclo che si autoalimenta e può facilmente farci sentire sopraffatti. Grazie alle *ICT* siamo entrati nell'*era dello zettabyte*. La nostra è la prima generazione a sperimentare l'ondata di *zettabyte* e a coniare un termine per descrivere lo tsunami di dati che ci sommerge. In altri contesti, si parla anche di *big data*[120].

I *big data* e l'*Internet of Things* (IoT) sono al centro dell'era degli algoritmi, rappresentando innovazioni che offrono nuove opportunità, ma anche nuove sfide per la società. La Commissione europea, nella comunicazione del 2 luglio 2014 "*Verso una florida economia basata sui dati*", definisce i *big data* come "grandi quantità di dati di tipo diverso prodotti a grande velocità da numerose fonti". Gestire questi dati variabili e in tempo reale richiede nuovi strumenti e metodi, come potenti processori, *software* e algoritmi. I *big data* si possono quindi descrivere come enormi volumi di dati, raccolti e detenuti da organizzazioni pubbliche e private, provenienti da fonti diverse e analizzati con algoritmi, tecniche di *data mining*, *software di big data analytics*, *machine learning* e *tecnologie specifiche*. Questa definizione è riportata

[119] Cfr. P. Gallo, *Big data e diritto allo sfruttamento economico dei dati personali* in Massimo D'Auria (a cura di), *I problemi dell'informazione nel diritto civile, oggi,* Roma, I ed., 2022, p. 376-377.

[120] Cfr. L. Floridi, *La quarta rivoluzione come l'infosfera sta trasformando il mondo,* Milano, I ed., 2017.

anche nell'*Opinion 03/2013 on purpose limitation*, adottata il 2 aprile 2013 dall'*Article 29 Data Protection Working Party*.

I *big data* sono costituiti dalle eterogenee *tracce digitali* che derivano dalle nostre interazioni online: dati forniti volontariamente sulle piattaforme *online* (*Google, Amazon, Facebook*); dati scambiati in cambio di benefici (raccolte punti, tessere fedeltà, *app* che offrono sconti); dati forniti consapevolmente o meno (*GPS* del telefono); dati registrati automaticamente (*cookies*) o derivati da altri dati; dati raccolti dai poteri pubblici e talvolta resi disponibili come *open data*; e i cosiddetti dati residui (*data exhaust*), cioè le *tracce digitali* lasciate dalle azioni e comportamenti online, che possono essere utilizzate per altri servizi e prodotti (ad esempio, gli errori di digitazione nei motori di ricerca usati per migliorare i correttori ortografici). Le soluzioni di intelligenza artificiale si basano anch'esse su enormi quantità di dati e su algoritmi che li utilizzano per funzionare. I *big data* sono onnipresenti e costituiscono anche il *cuore* dell'*Internet of Things* (IoT)[121].

La prima manifestazione concreta del concetto di *Internet delle cose* (*IoT*) avvenne nel 1982, quando un distributore di Coca Cola modificato presso l'Università Carnegie Mellon di Pittsburgh divenne il primo dispositivo connesso a Internet capace di inviare informazioni. Tuttavia, il termine "*Internet of Things*" fu coniato per la prima volta nel 1998 dall'ingegnere inglese Kevin Ashton per descrivere la connessione di oggetti fisici a Internet. Oggi possiamo dire che l'*Internet of Things* comprende tutte quelle reti di dispositivi connessi – ovvero una famiglia di tecnologie innovative – capaci di acquisire informazioni dall'ambiente, elaborarle e quindi agire di conseguenza producendo effetti appropriati. Una caratteristica fondamentale degli "*oggetti*" (*things*) è la capacità di comunicare direttamente o indirettamente con la rete Internet. Questo permette di gestire grandi volumi di dati generati dai sensori, che non potrebbero essere memorizzati

[121] Cfr. F. Faini, *Big data e internet of things: data protection e data governance alla luce del regolamento europe* in G. Cassano, V. Colarocco, G. B. Gallus, F. P. Micozzi, *Il processo di adeguamento al GDPR aggiornato al d lgs 10 agosto 2018 n.101,* Milano, 2018, p. 260-261.

localmente. Tali informazioni diventano accessibili tramite servizi Internet o Web, consentendo ad altre applicazioni di accedervi e interagire in base ai dati ricevuti[122].

Una definizione a livello giuridico di *Internet of Things* (IoT) è fornita dal Garante per la protezione dei dati personali nella deliberazione del 26 marzo 2015, che ha avviato una consultazione pubblica sul tema. Secondo questa definizione, l'*IoT* riguarda infrastrutture in cui numerosi sensori sono progettati per registrare, elaborare e memorizzare dati localmente o interagendo tra loro, sia a breve distanza tramite tecnologie a radiofrequenza (come *RFID* e *Bluetooth*), sia attraverso una rete di comunicazione elettronica. Questi dispositivi non includono solo *computer* e *smartphone* tradizionali, ma anche oggetti di uso quotidiano ("*things*"), come dispositivi indossabili (*wearables*), dispositivi di automazione domestica (domotica) e sistemi di georeferenziazione e navigazione. Questi strumenti raccolgono e gestiscono dati relativi ai comportamenti, alle abitudini, alle preferenze e allo stato di salute degli utenti, spesso senza che questi ne siano consapevoli, permettendo così la creazione di profili dettagliati.

Analogamente, la Commissione europea, nella comunicazione del 18 giugno 2009 "*L'internet degli oggetti — Un piano d'azione per l'Europa*", descrive l'*IoT* come una rete di oggetti che possono avere un proprio indirizzo IP, essere inseriti in sistemi complessi e utilizzare sensori per ottenere informazioni dall'ambiente (ad esempio, prodotti alimentari che registrano la temperatura durante la catena di approvvigionamento) o dispositivi di comando per interagire con l'ambiente (come valvole dell'aria condizionata che reagiscono alla presenza di persone). Da queste definizioni emerge che nell'*IoT* gli oggetti non sono solo connessi alla rete, ma anche tra loro, permettendo così lo scambio e l'incrocio di dati prodotti. Questo evidenzia l'ampiezza e la varietà degli oggetti coinvolti nell'*IoT*, che coprono settori come la domotica, la robotica, l'industria automobilistica, il biomedicale, il monitoraggio industriale, la rilevazione di eventi avversi e le *smart home*. I dati su cui si basa l'*IoT* sono *big data*, poiché l'*IoT* consente di "*digitalizzare*" tutto ciò che ci circonda, inserendo sensori e chip negli oggetti e producendo così enormi quantità di dati che

[122] Cfr. L. Vizzoni, *Domotica e diritto. La Smart Home tra regole e responsablità*, Milano, I ed., 2021, p. 10-11.

possono essere analizzati da potenti algoritmi. Le caratteristiche intrinseche dell'*IoT* e dei *big data* rendono opportuno trattarli insieme, poiché sono strettamente collegati anche nelle problematiche giuridiche che pongono: entrambi si basano su dati, che presentano elementi specifici da analizzare, e su algoritmi capaci di estrarre conoscenza e valore[123].

Le applicazioni dell'*Internet delle cose* (*IoT*) interessano molteplici settori, a partire dall'*industria 4.0*, e sono sempre più integrate con l'uso di piattaforme che consentono di connettere e controllare i dispositivi da remoto, memorizzare e analizzare i dati raccolti, monitorare e gestire gli oggetti connessi. Riguardo ai dati personali raccolti dagli oggetti connessi, diventa oggi cruciale non solo la nozione di interconnessione, ma anche quella di interoperabilità tra i sistemi informatici. La tendenza attuale è lo sviluppo di *multipiattaforme* che permettono il controllo di dispositivi *smart* di diversi fornitori e marche da un unico punto di accesso. Particolarmente significativo è l'accordo tra *Amazon*, *Apple* e *Google*, generalmente non inclini alle alleanze, per la creazione di un protocollo unitario per la casa connessa, grazie al quale tutti i dispositivi potranno essere controllati con *Alexa*, *Siri* e *Google Assistant*. In questo contesto, le implicazioni legate alla sicurezza e all'interoperabilità delle architetture *IoT*, che stanno diventando sempre più pervasive, attireranno inevitabilmente l'attenzione degli studiosi[124].

L'*Internet delle Cose* (*IoT*) è composto da una serie di tecnologie che, a seconda del tipo di oggetti coinvolti, possono essere categorizzate in etichette specifiche. Ad esempio, il cosiddetto *quantified self* comprende quelle tecnologie che monitorano il comportamento del corpo umano, raccogliendo dati utili per agire in maniera mirata. Il termine *smart home* si riferisce alla connessione dello spazio domestico alla rete, mentre la *smart city* rappresenta un'estensione su scala urbana, digitalizzando l'intera città. Ogni ambito menzionato mette in luce un diverso aspetto della sfida posta dal mondo intelligente. Inoltre, a livello personale, l'*IoT* include anche sensori biometrici

[123]Cfr. Faini, *Big data e internet of things: data protection e data governance alla luce del regolamento europeo* cit., pp. 260-261.
[124] Cfr. Vizzoni, *Domotica e diritto. La Smart Home tra regole e responsablità* cit., pp. 12-13.

indossabili, dispositivi che raccolgono dati biometrici e li rendono disponibili per l'osservazione e l'analisi in rete[125].

I *big data*, che costituiscono anche la base dell'*Internet of Things* (*IoT*), si distinguono per alcune caratteristiche specifiche legate alla loro vastità. Innanzitutto, c'è la varietà, che riguarda l'eterogeneità nei tipi e nei formati dei dati. Questi dati provengono da fonti diverse e includono dati strutturati, non strutturati, dati generati dagli utenti e dati personali. Poi c'è il volume, che si riferisce alla capacità di acquisire, memorizzare, accedere ed elaborare enormi quantità di dati. Un'altra caratteristica fondamentale è la velocità, ossia la capacità di acquisire e analizzare i dati in tempo reale o a una velocità molto elevata. Questa rapidità evidenzia due ulteriori aspetti importanti: la dinamicità dei dati e l'importanza del tempo, dato che i dati possono diventare obsoleti molto rapidamente. Oltre a queste tre caratteristiche principali, spesso se ne considerano altre due. Il valore si riferisce all'importanza e all'utilità complessiva dei *big data*. La veracità, invece, riguarda la qualità e l'accuratezza delle analisi effettuate sui dati. Queste caratteristiche insieme formano il paradigma delle 3, 4 o 5 "V" dei *big data*: volume, velocità, varietà, valore e veracità[126].

Attualmente, l'*IoT* rappresenta la prova più evidente del desiderio umano di misurare e controllare il mondo. Utilizzando dispositivi di rilevamento, l'*IoT* consente di quantificare i processi vitali a ogni livello, trasformandoli in dati digitali da analizzare.

È importante considerare gli effetti prodotti ogni volta che queste tecnologie vengono impiegate e nuovi dati vengono generati. L'*IoT* offre opportunità illimitate, tuttavia, esistono anche preoccupazioni significative, soprattutto riguardo alla sicurezza. Questo include sia la sicurezza strutturale dei dispositivi utilizzati sia la protezione dei dati custoditi al loro interno. Alcuni dispositivi, come i *router*, sono spesso soggetti ad attacchi informatici e non vengono sempre aggiornati periodicamente. Inoltre, i sensori dell'*IoT* rilevano dati, li trasmettono in rete e li

[125] Cfr. F.Bucci, *IoT e privacy:il problema della logica plug and play* in Iusinitinere.it, pubblicato il 7.04.2021, consultato il 21.05.2024, p. 3.
[126] Cfr. Faini, *Big data e internet of things: data protection e data governance alla luce del regolamento europeo* cit., pp. 261-262.

archiviano digitalmente; tuttavia, spesso non è chiara la natura dei dati raccolti e dove queste informazioni vengano memorizzate nella rete. Le problematiche relative all'*IoT* sono molteplici e includono questioni comuni nel dibattito sulle nuove tecnologie, come la privacy, la profilazione e la sicurezza[127].

«*Insomma, dagli smartphone con fotocamere multiple agli Assistenti digitali intelligenti per la casa, tutto fa capire che la tecnologia è in continuo movimento e che per il suo sviluppo è vitale la capacità di conoscere sempre più a fondo l'essere umano, le sua abitudini e i suoi comportamenti*»[128]. Da quanto Francesco Pizzetti scrisse queste parole è passato un po' di tempo, e, in effetti, anche grazie ai dati appresi da questi oggetti, la tecnologia si è evoluta ancora da quel momento. Si sottolinea così come questi oggetti raccolgano dati anche con lo scopo di migliorarsi continuamente, comportando una sorta di *circolo virtuoso* o *vizioso*, a seconda della prospettiva di osservazione del fenomeno.

2.2.1 *Smart assistant: focus sulla domotica*

Negli ultimi anni, lo sviluppo delle tecnologie digitali integrate nella vita di tutti i giorni ha portato a una vasta diffusione degli *smart assistant*. Questi *software*, grazie al *machine learning*, cioè a sistemi di apprendimento basati su algoritmi di intelligenza artificiale, possono comprendere il linguaggio naturale delle persone e interagire con loro. Questa interazione può servire a rispondere a diverse esigenze, come fissare appuntamenti, impostare sveglie, *timer* e promemoria, riprodurre musica o notizie, fornire previsioni del tempo e del traffico, oppure a eseguire specifiche azioni, come accendere una luce, avviare un elettrodomestico o regolare la temperatura di una casa. Il loro basso costo, la frequente preinstallazione nei dispositivi e la facilità d'uso hanno contribuito a diffondere e a favorirne l'utilizzo. Possono essere installati su una varietà di supporti: dagli *smart speaker* presenti nelle abitazioni e in altri ambienti come i luoghi di lavoro, fino alle automobili, ai dispositivi indossabili, e ai dispositivi più comuni come *smartphone*, *computer* e

[127] Cfr. F.Bucci, *IoT e privacy:il problema della logica plug and play* in Iusinitinere.it, pubblicato il 7.04.2021, consultato il 21.05.2024, p. 3-4.
[128] V. F. Pizzetti, *L'intelligenza artificiale che ci spia a casa: quali rischi e soluzioni per la privacy* in Agenda Dgitale, pubblicato il 4.07.2018, consultato il 20.05.2024.

tablet. In particolare, questi assistenti possono anche facilitare lo svolgimento di attività quotidiane per persone con autonomia ridotta[129].

Per formulare una prima definizione, possiamo fare riferimento al linguaggio comune, secondo cui la domotica è la disciplina che si occupa dell'applicazione dell'elettronica e dell'informatica ai dispositivi e agli impianti utilizzati nelle abitazioni, automatizzandoli. Il termine deriva dal neologismo francese *domotique*, una contrazione della parola greca *domos* (casa, costruzione) e di *automatique* (automatica), significando letteralmente *casa automatica*. In sostanza, la domotica può essere vista come la scienza che studia e applica tecnologie per migliorare la vita domestica attraverso sistemi programmabili dall'utente o parzialmente autonomi; una scienza che finora ha avuto poco confronto con gli studi giuridici. Le applicazioni della domotica dimostrano concretamente come semplici oggetti domestici possano essere connessi e interagire tra loro e con l'ambiente circostante. Gli studi specialistici fanno generalmente riferimento a questo aspetto. Tra le numerose funzioni caratteristiche di un ambiente *domotico* si possono includere, ad esempio, l'accensione e lo spegnimento di luci, riscaldamento o condizionamento, il controllo di porte, cancelli, tapparelle, elettrodomestici, parametri ambientali e atmosferici, oltre alla gestione di un sistema di allarme.

La specificità della domotica risiede nella gestione coordinata, integrata e computerizzata degli impianti tecnologici (climatizzazione, distribuzione di acqua, gas ed energia, impianti di sicurezza), delle reti informatiche e delle reti di comunicazione. Le possibili aree di automazione di una casa includono la gestione dell'ambiente (microclima e requisiti energetici, con rilevazione delle presenze), degli apparecchi domestici e dell'impianto elettrico, l'automazione delle aperture, i sistemi di protezione dalle intrusioni con monitoraggio a distanza degli ambienti, il rilevamento di eventi che interessano l'ambiente domestico e la connessione con servizi di assistenza, come soccorso medico o vigilanza[130].

[129]Cfr. L.Vizzoni, *Smart assistant e dati personali: quali rischi per gli utenti?* in Media Laws, n.2, 2020, consultato il 17.05.2024, p. 108.

[130]Cfr. Vizzoni, *Domotica e diritto. La Smart Home tra regole e responsablità* cit., pp. 7-8.

Anche nel campo della domotica, semplificando, si può affermare che il funzionamento ottimale delle apparecchiature delle *smart home*, inclusa la capacità di registrare, archiviare, trasferire e utilizzare informazioni, trae grande beneficio dallo sviluppo degli algoritmi di intelligenza artificiale. Un elemento chiave dell'IA applicata alla domotica, soprattutto per quanto riguarda gli *smart speaker*, ma anche per dispositivi non strettamente domotici come *smartwatch* e *smartphone*, è la ricerca vocale. Quando gli utenti lanciano ricerche vocali, inviano segnali ai sistemi di IA, che utilizzano questi *input* per migliorarsi continuamente attraverso tecniche di *machine learning*, fornendo risposte sempre più precise. L'intelligenza artificiale, a sua volta, si basa sui dati personali e altre informazioni provenienti dalla nostra vita quotidiana, che è intrisa di interazioni digitali con l'ambiente circostante. Lo sviluppo di algoritmi avanzati di IA ha reso possibile la creazione di sistemi domestici parzialmente o totalmente autonomi, capaci di apprendere e monitorare le abitudini degli abitanti. Questi sistemi migliorano costantemente nel tentativo di adattare i servizi offerti alle esigenze degli individui[131].

Per fare questo, gli assistenti vocali raccolgono quasi ininterrottamente dati personali non solo dell'utente principale, ma anche di chiunque si trovi nell'ambiente circostante. Inoltre, gli *smart assistant* possono sfruttare le funzionalità offerte dall'*Internet delle cose* (*IoT*), utilizzando vari dispositivi, cioè le *things* che integrano programmi di assistenza vocale intelligente, per raccogliere informazioni e migliorare i servizi offerti. Questi assistenti vocali sono in grado di comunicare con altri dispositivi *IoT*, come *smartwatch*, *smart TV*, sistemi di controllo remoto o di videosorveglianza, ampliando così la capacità di raccolta, incrocio e diffusione dei dati personali[132].

La prima fu *Amazon Echo*, con dimensioni paragonabili a un disco da hockey o un portapillole, a seconda dei punti di vista. Questo dispositivo era essenzialmente un *chatbot*: un robot in grado di chattare con le persone, pubblicizzato come una presenza interattiva attivabile a comando, capace di sostenere una conversazione o di fornire risposte coerenti quando qualcuno iniziava a parlare con esso. Era concepito

[131] Cfr. Vizzoni, *Domotica e diritto. La Smart Home tra regole e responsablità* cit., p. 29-30.
[132] Cfr. Vizzoni , *Smart assistant e dati personali: quali rischi per gli utenti?* cit., p. 108.

per alleviare la solitudine o fornire una compagnia costante. Inoltre, il dispositivo fungeva anche da assistente digitale *intelligente*, predisposto per controllare le apparecchiature domestiche, specialmente man mano che la connessione Internet tra questi dispositivi si sviluppava. Nel frattempo, offriva *playlist* musicali, collegamenti radio e forme semplificate di domotica come l'accensione e lo spegnimento delle luci, oltre ad altre integrazioni con vari dispositivi domestici[133].

Il paradigma è cambiato: non si tratta più solo di frigoriferi intelligenti, ma di una casa interamente connessa. Oggetti come lampadine, termostati, sensori di fumo, stazioni meteorologiche, lavatrici e acquari sono controllabili da remoto tramite Internet. Come rilevato dal Gruppo Articolo 29, i dispositivi dotati di sensori possono rilevare la presenza e i movimenti degli utenti e attivare azioni predeterminate, come accendere luci o regolare la temperatura. Molti dispositivi domotici trasmettono dati ai produttori o a terzi, anche automaticamente, riguardo a necessità di manutenzione o preferenze degli utenti. Questo comporta rischi per la privacy, soprattutto quando i dati vengono condivisi con terzi senza la piena consapevolezza degli utenti. La presenza pervasiva di sensori solleva sfide complesse per la protezione della privacy e dei dati personali, trasformando Internet in una *nuova dimensione* in cui si esercitano diritti e libertà, ma si verificano anche discriminazioni[134].

Esistono dei rischi nascosti, principalmente per quanto riguarda i dati personali, anche nelle soluzioni domotiche che utilizzano l'architettura *IoT*. La casa è uno degli ambienti più dinamici per l'*IoT* e la diffusione di modelli contrattuali *pay for use* o *pay for performance*, che permettono pagamenti dilazionati per l'acquisto di dispositivi *smart* per edifici, ne accentuerà ulteriormente questa caratteristica. Non sorprende che la domotica sia stata citata dal Garante per la protezione dei dati personali nelle premesse alla deliberazione del 26 marzo 2015 durante l'avvio della consultazione pubblica sull'*Internet delle cose*, dove l'automazione domotica è elencata tra i dispositivi che costituiscono le fonti dell'infrastruttura di sensori, che interagiscono per registrare, elaborare e memorizzare dati[135].

[133] Cfr. Pizzetti, *L'intelligenza artificiale che ci spia a casa: quali rischi e soluzioni per la privacy* cit.
[134] Cfr. Vizzoni, *Domotica e diritto. La Smart Home tra regole e responsablità* cit., p. 16-17.
[135] Cfr. Vizzoni, *Domotica e diritto. La Smart Home tra regole e responsablità* cit., p. 14.

2.2.2 *Self-driving cars*

Nell'ambito dell'*Internet of Things*, uno dei settori in più rapida crescita è quello automobilistico, grazie all'introduzione dei veicoli autonomi, capaci di svolgere le principali funzioni di un'auto tradizionale in modo automatico. Si prevede che entro vent'anni circa 250 milioni di veicoli saranno connessi in rete, e il mercato automobilistico, basato in gran parte sul *cloud computing*, crescerà esponenzialmente, fino a quadruplicarsi. Entro il 2025, si raggiungerà un livello di automazione tale (livello 3 dello standard SAE J3016) che il conducente non dovrà monitorare costantemente il veicolo, anche se dovrà essere sempre pronto a riprenderne il controllo. I veicoli autonomi devono essere connessi in rete per comunicare tra loro, e ciò include il settore automobilistico nell'*Internet of Things*[136].

I veicoli autonomi sono estremamente complessi, poiché integrano sia componenti *hardware*, come sensori (telecamere, radar, lidar e sensori a ultrasuoni) che raccolgono informazioni sull'ambiente circostante, inclusa la posizione degli altri veicoli, la segnaletica stradale e le condizioni meteorologiche; sia *software* avanzati, tra cui sistemi di intelligenza artificiale e algoritmi di *machine learning*, che analizzano i dati dei sensori per rilevare e rispondere in tempo reale alle situazioni stradali. La ricerca scientifica e tecnologica nel campo della mobilità intelligente punta a sviluppare veicoli sempre più autonomi, riducendo progressivamente il ruolo attivo del conducente umano, per permettere ai veicoli di operare in totale autonomia nel traffico. Questo processo è ben illustrato dalla classificazione dei livelli di autonomia della *SAE* (*Society of Automotive Engineers*), che descrive come cambia il rapporto tra veicolo e conducente man mano che il veicolo diventa capace di eseguire più funzioni senza intervento umano. Il livello 0 indica veicoli senza alcuna automazione, dove il conducente controlla completamente il veicolo. Al livello 1, alcune funzioni assistono il conducente, come il parcheggio assistito, il cruise control e il mantenimento della corsia, ma il conducente rimane il responsabile principale della guida. Il livello 2 prevede un'automazione parziale, con il veicolo capace di eseguire autonomamente alcune manovre, richiedendo comunque la supervisione

[136] Cfr. M. C. Gaeta, *La protezione dei dati personali nell'internet of things: l'esempio dei veicoli autonomi* in *Il diritto dell'informazione e dell'informatica*, anno XXXIV, n.1, 2018, pp. 149-150.

costante del conducente. Il livello 3, detto automazione condizionata, consente al veicolo di gestire autonomamente alcune funzioni di guida, ma richiede l'intervento umano in situazioni di emergenza o di scarsa visibilità. Il livello 4 rappresenta un'automazione elevata, dove il veicolo può gestire autonomamente la maggior parte delle fasi della guida, necessitando l'intervento umano solo in situazioni specifiche. Infine, il livello 5 indica l'automazione totale: il veicolo è completamente autonomo, senza bisogno di intervento umano o della presenza di un conducente, operando in tutte le fasi della guida in modo completamente indipendente[137].

Le connessioni dei veicoli automatizzati, detti anche *connected vehicles*, sono di tre tipi principali. La prima è la *Vehicle to Device Communications* (V2D), che permette ai veicoli di comunicare con dispositivi come *smartphone*, *smartwatch*, *tablet* e *computer* tramite *app* dedicate. La seconda è la *Vehicle to Infrastructure Communications* (V2I), che riguarda la comunicazione tra veicoli e infrastrutture come semafori e dispositivi di controllo della velocità. La terza e più avanzata è la *Vehicle to Vehicle Communications* (V2V), che richiede veicoli completamente autonomi o con un alto livello di automazione. La connessione tra veicoli richiede che essi siano almeno parzialmente automatizzati, e il livello di comunicazione è direttamente proporzionale al grado di automazione. Tuttavia, la connessione è solo uno degli elementi necessari per la completa automazione del veicolo.

L'*IoT* è una delle innovazioni più significative dell'*Information Technology*, ma presenta anche numerose sfide, specialmente nel settore automobilistico, dove è necessaria una regolamentazione adeguata. Una delle principali problematiche è la responsabilità in caso di incidenti causati da malfunzionamenti dei veicoli autonomi. Inoltre, d'interesse per questo elaborato, con la riforma europea sulla protezione dei dati, è importante affrontare la tutela dei dati personali trasmessi dai veicoli autonomi e la profilazione degli utenti, che spesso non sono consapevoli delle possibili conseguenze negative[138].

[137] Cfr. T. De Mari Casareto dal Verme, *Rischio da circolazione stradale, R.C. auto e veicoli a guida autonoma* in BioLaw Journal-Rivista di Biodiritto, n.3/2023, 277-278.
[138] Cfr. M. C. Gaeta, *La protezione dei dati personali nell'internet of things: l'esempio dei veicoli autonomi* cit., pp. 151-152.

L'introduzione dei veicoli autonomi nella società apporterà numerosi benefici sociali ed economici, tra cui: un significativo aumento della sicurezza stradale, con una possibile riduzione degli incidenti fino al 90%; maggiore efficienza del traffico grazie alla comunicazione tra i veicoli e l'infrastruttura stradale, che ottimizzerà il flusso del traffico e ridurrà i tempi di percorrenza; riduzione delle emissioni dovuta all'elettrificazione dei veicoli; maggiore accessibilità per anziani, disabili e minori; risparmio economico su costi di carburante, parcheggio e sanzioni stradali; e la creazione di nuovi posti di lavoro nei settori tecnologico e ingegneristico. Un vantaggio particolarmente rilevante è il miglioramento della qualità della vita grazie al tempo libero guadagnato in auto. Con i veicoli autonomi, il tempo che oggi viene dedicato alla guida potrà essere impiegato per altre attività. Questo significa che i passeggeri potranno lavorare, studiare o semplicemente riposarsi durante i loro spostamenti, trasformando il viaggio in un momento produttivo o rilassante, anziché un obbligo stressante[139].

Quest'ultimo aspetto fa riflettere su di una cosa: già oggi le auto raccolgono molti dati personali su cosa si fa in auto e anche su come si guida, quando le auto non si dovranno più guidare e questo tempo libero che sarà trascorso su di esse sarà speso per molte attività diverse, si può ipotizzare che i dati raccolti sulle auto potranno essere analoghi ai dati e alle modalità con cui vengono raccolti di cui si parla nell'ambito della domotica?

2.2.3 *Robotica*

Il termine *robotica*, introdotto da Isaac Asimov nel 1941, si riferisce alla progettazione e costruzione di varie macchine, tra cui *robot* soldati, chirurghi, sistemi di trasporto automatizzati e applicazioni industriali. Questo campo interdisciplinare integra informatica, cibernetica, matematica, meccanica, elettronica, neuroscienze, biologia e scienze umane. Data la complessità, c'è dibattito sulla definizione di *robot* e caratteristiche come *autonomia*, *adattività* e *interattività*. La robotica è vista come una branca dell'IA che crea macchine capaci di *sentire, pensare e agire*. Definizioni

[139] Cfr. T. De Mari Casareto dal Verme, *Rischio da circolazione stradale, R.C. auto e veicoli a guida autonoma* in BioLaw Journal-Rivista di Biodiritto, n.3/2023, 278-279.

specifiche, come quella ISO 8373, descrivono un *robot* come un manipolatore multiuso, programmabile e controllato automaticamente. L'autonomia dei *robot*, come nei sistemi aerei senza pilota, implica la capacità di comprendere e rispondere a comandi complessi, con stime sull'intelligenza artificiale che variano tra cinque e quindici anni. Il problema attuale è l'imprevedibilità delle azioni dei *robot* a causa della loro interattività, autonomia e adattabilità. Questo richiede una notevole capacità computazionale e solleva questioni di responsabilità giuridica nelle applicazioni industriali, militari e di servizio. La robotica di servizio si divide in professionale e domestica, con applicazioni che includono ispezione, costruzione, logistica, medicina, difesa, sicurezza e intrattenimento. In ambito *HRI* (*Interazione Uomo-Robot*), si distinguono approcci centrati sull'uomo, che considerano l'accettabilità dei *robot*, e sul *robot*, visto come entità autonoma. Queste prospettive sollevano questioni di responsabilità, soprattutto in caso di incidenti[140].

La letteratura tecnologica ed economica attuale descrive con crescente frequenza come la ricerca sulle macchine intelligenti e la robotica abbiano raggiunto livelli che un tempo erano solo immaginati nella fantascienza. All'inizio della quarta rivoluzione industriale, le applicazioni più avanzate della robotica si trovavano nei settori industriali, dove hanno progressivamente trasformato il processo produttivo fordista, sostituendo gli esseri umani con macchine sempre più capaci di svolgere compiti con una precisione, velocità e durata ineguagliabili dall'uomo. I processi lavorativi pericolosi per l'uomo sono stati delegati alle macchine, riducendo notevolmente il rischio di infortuni per i lavoratori. Con il tempo, la robotica si è estesa oltre i settori industriali, coinvolgendo progressivamente tutti i sistemi sociali, produttivi e le singole persone. Oggi, le applicazioni robotiche influenzano significativamente le attività umane in vari ambiti: ludico, relazionale, comunicativo, lavorativo, con impatti su tecnologia, economia, etica, diritto e comunicazione[141].

[140] Cfr. U. Pagallo, *Introduzione alla robotica di servizio in* C. Artusio, M. A. Senor (a cura di), *The law of service robot Ricognizione dell'assetto normativo rilevante nell'ambito della robotica di servizio: stato dell'arte e prime raccomandazioni di policy in una prospettiva multidisciplinare*, Politecnico di Torino, 4.12.2015.

[141] Cfr. P. L. Di Viggiano, *Etica, robotica e lavoro: profili d'informatica giuridica* in Revista Opinião Jurídica (Fortaleza), n.22, 2018, p. 249-250.

Robot, automi, androidi e *cyborg* sono termini con significati distinti. Per quanto riguarda l'intelligenza artificiale, la letteratura offre varie definizioni basate in alcuni casi sulla capacità di percepire l'ambiente e agire di conseguenza, e in altri sulla presenza di funzioni cognitive umane, come l'apprendimento e la risoluzione dei problemi. Tra le definizioni più note, quella di Ronald C. Arkin descrive il robot intelligente come "*a machine that is able to extract information from its environment and use knowledge about its world to move safely in a meaningful and purposeful manner".* Schank R.C., invece, sottolinea che la questione principale dell'intelligenza artificiale è *"What do we know, and how do we get a machine to know it?*".

Il Parlamento Europeo ha chiesto alla Commissione di proporre definizioni europee comuni per *sistemi ciberfisici*, *sistemi autonomi*, *robot autonomi intelligenti* e le loro sottocategorie, specificando le caratteristiche che dovrebbe avere un robot intelligente: la capacità di acquisire autonomia tramite sensori e/o scambio di dati con l'ambiente (*interconnettività*) e l'analisi di tali dati; la capacità di autoapprendimento dall'esperienza e dall'interazione (*criterio facoltativo*); la forma del supporto fisico richiesto; l'adattamento del comportamento e delle azioni all'ambiente; e l'assenza di vita in termini biologici. È cruciale comprendere cosa sia un robot, come dimostra il fatto che tra le raccomandazioni del Parlamento Europeo vi è l'istituzione di un sistema di registrazione dei "*robot avanzati*" a livello dell'Unione Europea. Un *robot* non può acquisire informazioni come un cervello umano; uomo e *robot* imparano e applicano comportamenti in modo diverso; la conoscenza dei *robot* è dinamica e le loro reazioni dipendono principalmente da programmi e dati forniti dall'uomo, sebbene si evolvano grazie al continuo flusso di informazioni che ricevono, aumentando così la loro autonomia decisionale. Questo passaggio è cruciale: mentre le azioni e reazioni dei *robot* non sono automatiche, è evidente che, nei *robot* capaci di apprendere dall'esperienza, risultano incerte come quelle umane o animali. Maggiore è l'autonomia del *robot*, minore è il controllo umano sull'intelligenza artificiale, con conseguenze in termini di sicurezza. Questo

aspetto diventa decisivo considerando i molteplici settori in cui si applica la robotica, come quello sanitario, automobilistico, assistenziale e molti altri[142].

I *robot* sono sistemi intelligenti dotati di un corpo con attuatori e sensori e di un sistema di controllo che utilizza l'intelligenza artificiale per prendere decisioni funzionali al loro operato nello spazio di lavoro. La robotica espande le capacità dell'intelligenza artificiale permettendo l'esecuzione di compiti fisici, convertendo energia e compiendo azioni. Tecnologie avanzate come la robotica, l'intelligenza artificiale, il *machine learning* e il *cloud computing* stanno trasformando il modo di produrre beni e servizi. La vera innovazione futura risiederà nella diffusione dei *robot* nella vita quotidiana, rendendoli accessibili ai consumatori e non solo a personale specializzato. L'Italia, essendo uno dei principali produttori di robot al mondo, ha una posizione di grande competitività e potrà giocare un ruolo significativo in questa trasformazione. Oggi, i *robot* stanno diventando collaboratori diretti degli operai, come nel caso della robotica collaborativa, che, dal 2016, ha iniziato a trasformare il settore. Un ulteriore passo avanti è rappresentato dalla robotica indossabile, come gli esoscheletri industriali, che aiutano gli operai, riducendo lo sforzo fisico e i rischi per la salute, sostenendo il sollevamento dei carichi.

La robotica è fondamentale per ottimizzare i processi produttivi, ridurre i rischi lavorativi e minimizzare l'impatto ambientale di alcuni processi. L'integrazione di robot collaborativi e indossabili con l'intelligenza artificiale permette ai robot di adattarsi a situazioni impreviste attraverso l'apprendimento, superando i limiti delle regole preimpostate. Tuttavia, questa fusione solleva questioni etiche e legali, poiché rende il comportamento dei robot meno prevedibile e la responsabilità in caso di incidenti più difficile da determinare. Un aspetto ancora più avanzato è rappresentato dalle protesi cibernetiche e dalla bionica, dove la robotica e l'intelligenza artificiale si integrano direttamente nel corpo umano, supportando le funzioni fisiologiche con

[142] Cfr. G. Capilli, *Responsabilità e robot*, in G. Alpa, P. Zatti (a cura di), *La nuova giurisprudenza civile commentata,* anno XXXV, n.3, 2019, p. 622-623.

sistemi impiantabili. Oggi, i *robot* possono interagire con le persone, dalla robotica collaborativa e indossabile alle protesi di arti e ai sistemi impiantabili[143].

Classificare i *robot* come prodotti richiede necessariamente una valutazione del loro grado di autonomia decisionale. Alcuni studiosi hanno evidenziato che i primi *robot* erano macchine dotate di una certa autonomia e capaci di manipolare oggetti, cioè di spostare pezzi o utensili rigidi nello spazio, basandosi su istruzioni memorizzate o fornite al momento. Tra la fine degli anni '50 e l'inizio degli anni '60, è stato creato il primo robot programmabile e solo negli anni '80 la robotica si è sviluppata parallelamente alla cibernetica. Come indicato nella Risoluzione del 2017[144], "l'autonomia di un robot può essere definita come la capacità di prendere decisioni e attuarle nel mondo esterno, indipendentemente da un controllo o un'influenza esterna; tale autonomia è di natura puramente tecnologica e il suo livello dipende dalla complessità con cui è stata progettata l'interazione del robot con l'ambiente". Pertanto, è essenziale riflettere sulla definizione di prodotto contenuta nella direttiva comunitaria e chiedersi se possa includere i *robot* o se sia necessaria una modifica legislativa. Finora i robot sono stati considerati prodotti, ma oggi si tratta di *prodotti* evoluti che hanno acquisito capacità di adattamento, prendono decisioni autonomamente e non richiedono l'intervento umano, se non nella fase di progettazione, ideazione e configurazione[145].

Grazie alla collaborazione delle neuroscienze cognitive, lo sviluppo delle intelligenze artificiali sembra poter raggiungere obiettivi estremamente ambiziosi nella creazione di una *Super-intelligenza*. Fino a poco tempo fa, lo studio della mente umana e della robotica erano settori completamente separati, con competenze e metodologie distinte. Tuttavia, oggi la distanza tra questi due campi di ricerca si sta costantemente riducendo, fino a quasi sovrapporsi, grazie ai progressi nella modellazione computazionale e nelle scienze cognitive. L'intersezione tra robotica e neuroscienze si manifesta principalmente attraverso due aspetti. Da un lato, c'è il

[143] Cfr. M. C. Carrozza, C. Oddo, S. Orvieto, A. di Minin, G. Montemagni, *AI: profili tecnologici Automazione e Autonomia: dalla definizione alle possibili applicazioni dell'Intelligenza Artificiale* in BioLaw-Rivista di Biodiritto, n, 3/2019, p. 245-246.

[144] Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL))

[145] Cfr. G. Capilli, *Responsabilità e robot* cit., pp.627-628.

tentativo di imitare il cervello umano e i suoi meccanismi di pianificazione e esecuzione delle azioni, al fine di sviluppare un modello artificiale funzionale delle aree cerebrali coinvolte nella visione e nell'azione motoria. Dall'altro lato, c'è l'obiettivo di utilizzare macchine intelligenti per approfondire la comprensione della mente umana, contribuendo così a risolvere il mistero della sua funzione e struttura[146].

È essenziale classificare con maggiore precisione le macchine intelligenti per distinguere chiaramente tra *robot* controllati esternamente e quelli capaci di autodeterminazione, una caratteristica che influisce su aspetti giuridici, sociali, etici ed economici. Una possibile soluzione consiste nel valutare i *robot* in base ai gradi di libertà tecnici, alle funzioni svolte nelle applicazioni specifiche e a una classificazione per livelli di autonomia. Questa classificazione dovrebbe partire da un livello base fino a definire il livello massimo, che descrive la capacità decisionale autonoma e le variabili applicative correlate. Il livello più avanzato di autonomia, proposto dal Gruppo di ricerca su *IoT* dell'Università Uniterma Sapienza di Roma, è il livello 9. Questo livello descrive *robot* con autonomia totale, capacità di formulare pensieri complessi, esercitare autocontrollo e apprendere profondamente (*deep learning*) anche dai propri errori, non solo attraverso *input* esterni. Ogni livello di questa scala di autonomia include e migliora le caratteristiche del livello precedente, rappresentando un modello evolutivo[147].

2.3 **IA generative**

L'intelligenza artificiale generativa si basa generalmente su modelli di base, cioè su modelli di intelligenza artificiale addestrati con enormi quantità di dati. Questi modelli riescono a imparare la distribuzione dei dati di addestramento, analizzarne la probabilità e generare nuovi contenuti che rispecchiano le caratteristiche più comuni dei dati originali. I modelli di base possono essere utilizzati tramite interfacce conversazionali oppure tramite *API* (*Application Programming Interface*), che gli sviluppatori integrano nel loro codice. Anche se l'IA generativa può spaziare dalla

[146] Cfr. M.B. Magro, *Robot cyborg e intelligenze artificiali* in A. Cadoppi, S. Canestrari, A. Manna, M. Papa, *Cybercrime,* Milano, I ed, 2019, pp. 1185-1186
[147] Cfr. Di Viggiano, *Etica, robotica e lavoro: profili d'informatica giuridica* cit., p. 252.

generazione di codice alla progettazione di nuove proteine, i modelli di base hanno trovato particolare applicazione nel campo del linguaggio naturale e delle immagini. Tra gli esempi più noti ci sono i modelli creati dalla società statunitense *OpenAI*: il primo è *GPT-4* (Generative Pre-trained Transformer 4), utilizzato per *ChatGPT* (la versione 4, disponibile a pagamento, è multimodale e risponde a input sia testuali che visivi, mentre la versione base comprende solo input testuali e utilizza il modello 3.5). Il secondo è *DALL·E 3*, un modello per la generazione di immagini[148].

Il funzionamento di un *chatbot*, come *Chat GPT*, è abbastanza semplice: l'utente pone una domanda e il sistema ricerca informazioni (disponibili su Internet), seleziona quelle rilevanti e infine genera una risposta in forma di testo. Questo modello si è dimostrato adatto all'automazione, essendo in grado di fornire risposte dettagliate e contestualizzate, anche in presenza di domande molto complesse[149].

Google ha rilasciato diversi modelli di base per l'AI generativa, tra cui *LaMDA* (*Language Model for Dialogue Applications*), *Bert* (*Bidirectional Encoder Representations from Transformers*), *PaLM 2* (*Pathways Autoregressive Language Model*) e *Gemini*. Quest'ultimo, anch'esso multimodale, è alla base della piattaforma *Gemini*, che ha sostituito *Bard* l'8 febbraio 2024. Un ulteriore esempio di modello di base per l'AI generativa è rappresentato dalla terza generazione dei modelli *Claude*, lanciati dalla società *Anthropic*. Come *GPT-4* e *Gemini*, questi modelli sono multimodali, capaci di gestire sia testo che immagini. Inoltre, secondo benchmark comparativi, *Claude 3* offre prestazioni superiori rispetto a *GPT-4* e *Gemini*. I modelli di base dell'IA generativa utilizzati per l'interpretazione del linguaggio naturale sono chiamati *Large Language Model* (*LLM*), una categoria che include anche *GPT-4* e *Gemini*. Dopo un pre-addestramento, i *LLM* possono essere adattati per esigenze specifiche, rendendoli adatti a una vasta gamma di applicazioni, come la traduzione o il riassunto.

---

[148] Cfr. C. Negri, *Come funziona l'AI generativa: significato e applicazioni* in Osservatori.net in collaborazione con Politecnico di Milano, ultimo aggiornamento 16.05.2024, consultato il 20.05.2024

[149] Cfr. G. Di Tonto, *Intelligenza artificiale e nuovi diritti. Il caso chat gpt* in Il bollettino di Clio, n.19, 2023.

Tra le prime architetture utilizzate per la generazione di contenuti troviamo le *GAN* (*Generative Adversarial Network*) e gli *AutoEncoder*. Tuttavia, questi modelli avevano difficoltà a gestire grandi quantità di testo. Questo ostacolo è stato superato con l'introduzione dei *Transformer*. Questa nuova capacità rappresenta una conquista significativa per l'intelligenza artificiale, resa possibile da tre fattori principali. Il primo fattore è la disponibilità di enormi quantità di dati, grazie a Internet, ai sensori *IoT* e al digitale in generale, che oggi forniscono una quantità di dati senza precedenti. Il secondo fattore è la grande evoluzione dei modelli e degli algoritmi alla base dell'IA, che hanno visto notevoli progressi. Il terzo fattore è l'avanzamento tecnologico degli *hardware* di nuova generazione, sempre più potenti e capaci di sfruttare appieno questa tecnologia. In questo contesto, è importante considerare che l'intelligenza artificiale generativa si basa su enormi quantità di dati elaborati da strutture molto complesse, come le reti neurali, e richiede quindi una notevole capacità computazionale.[150]

L'introduzione dei *Transformer* è stata una svolta per queste tecnologie e merita una digressione. Il *Transformer* è un'innovativa architettura di rete neurale progettata per superare le limitazioni dei modelli tradizionali basati su reti neurali ricorrenti (*RNN*) e convoluzionali (*CNN*), specialmente nei compiti di traduzione automatica e modellazione delle sequenze. A differenza dei modelli precedenti, il *Transformer* si basa esclusivamente su meccanismi di attenzione, eliminando completamente l'uso di ricorrenza e convoluzione. L'architettura del *Transformer* adotta una struttura *encoder-decoder*. L'*encoder* e il *decoder* sono entrambi formati da sei strati identici. Ogni strato dell'*encoder* è composto da due sotto-strati principali: un meccanismo di attenzione multi-testa (*Multi-Head Attention*) e una rete *feed-forward* completamente connessa. Il meccanismo di attenzione multi-testa consente al modello di focalizzarsi su diverse parti della sequenza in parallelo, migliorando la capacità di catturare le dipendenze a lungo termine. La rete *feed-forward* trasforma ogni posizione nella sequenza in modo indipendente attraverso una serie di operazioni lineari seguite da una funzione di attivazione *ReLU*. Per ogni sotto-strato, viene utilizzata una connessione residuale seguita dalla normalizzazione del livello, tecniche che aiutano

[150] Cfr. Negri, *Come funziona l'AI generativa: significato e applicazioni* cit.

a mantenere stabile il processo di addestramento migliorando il flusso del gradiente attraverso la rete. Il *decoder* ha una struttura simile all'*encoder*, ma con un sotto-strato aggiuntivo: l'attenzione mascherata. Questo meccanismo impedisce che le posizioni future influenzino la previsione della posizione corrente, garantendo che il modello generi l'*output* in modo auto-regressivo. Inoltre, il *decoder* utilizza un'attenzione multi-testa sulle uscite dell'*encoder*, permettendo al *decoder* di accedere alle informazioni elaborate dall'*encoder* e facilitando l'integrazione delle informazioni di *input* durante la generazione dell'*output*. Il *Transformer* utilizza un meccanismo chiamato attenzione a prodotto scalare (*Scaled Dot-Product Attention*), dove le *query*, le chiavi e i valori vengono proiettati in spazi dimensionali specifici. Il prodotto punto tra le *query* e le chiavi determina i pesi dell'attenzione, che vengono poi applicati ai valori per ottenere l'*output* finale.

L'attenzione multi-testa è un aspetto cruciale del *Transformer*. Questa tecnica esegue più operazioni di attenzione parallele, permettendo al modello di considerare simultaneamente diverse parti della sequenza. I risultati di queste operazioni parallele vengono quindi concatenati e proiettati in uno spazio dimensionale finale. Il Transformer offre numerosi vantaggi. Senza la necessità di ricorrenza, può elaborare tutti gli elementi della sequenza contemporaneamente, migliorando notevolmente l'efficienza computazionale. Nei compiti di traduzione automatica, ha raggiunto nuovi livelli di qualità, superando i modelli basati su *RNN* e *CNN*. Inoltre, può essere addestrato molto più rapidamente rispetto ai modelli ricorrenti, rendendolo estremamente pratico per applicazioni reali.

Il *Transformer* rappresenta una svolta significativa nel campo della traduzione automatica e della modellazione delle sequenze. La sua architettura, che sfrutta esclusivamente meccanismi di attenzione, consente una parallelizzazione efficiente e migliora la qualità delle previsioni[151].

Nel caso di *ChatGPT*, il funzionamento dell'algoritmo si basa sugli *embeddings*, vettori di significati associati a ogni parola. Questi vettori offrono una descrizione quantitativa della semantica di una sequenza di parole e del contesto in cui vengono

[151] Cfr. A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, L. Kaiser, I. Polosukhin, *Attention is all you need* in *Advances in Neural Information Processing Systems,* Long Beach (California), 30esima ed., 2017, *pp. 5998-6008.*

utilizzate. In sintesi, l'algoritmo di *ChatGPT* è una rete neurale che riceve gli *embeddings* di un testo in ingresso e restituisce gli *embeddings* del testo più probabile in risposta, basandosi sul corpus usato per l'addestramento della rete. La scelta degli *embeddings* influisce sul grado di esposizione individuale. Idealmente, questa scelta dovrebbe essere oggetto di dibattito pubblico, anziché essere lasciata esclusivamente agli sviluppatori della rete neurale[152].

L'uso di *chatbot* avanzati come quelli basati sui modelli di linguaggio *GPT* (*Generative Pre-trained Transformer*) può comportare diversi rischi. Un problema significativo è la diffusione di disinformazione. Questi *chatbot* vengono addestrati su una grande quantità di testo preso da *Internet*, che può includere informazioni errate o fuorvianti. Di conseguenza, le risposte generate possono sembrare accurate, ma essere, in realtà, false o non verificate, creando confusione tra gli utenti. Un altro aspetto preoccupante è la possibilità che i *chatbot* propaghino pregiudizi. Se i dati di addestramento contengono pregiudizi o stereotipi diffusi nella società, il modello può imparare a replicarli nelle risposte, contribuendo così a discriminazione o ingiustizie nella comunicazione con le persone. Questo è un problema serio, soprattutto in contesti dove l'equità e l'inclusività sono fondamentali.

Inoltre, c'è il rischio che i *chatbot* producano contenuti offensivi o inappropriati. A causa della loro capacità di generare testo in base agli *input* ricevuti, se stimolati da *input* inadeguati o maliziosi, potrebbero rispondere con messaggi volgari, offensivi o comunque inappropriati, danneggiando l'esperienza dell'utente e la reputazione di chi li utilizza. Un'altra questione è la mancanza di responsabilità. I *chatbot GPT* generano risposte senza una verifica o una comprensione approfondita delle informazioni. Questo solleva preoccupazioni riguardo a chi sia responsabile per le informazioni fornite, poiché le risposte del *chatbot* potrebbero essere attribuite erroneamente alla fonte o all'azienda che lo impiega, causando possibili malintesi o danni reputazionali. Infine, i *chatbot* basati su *GPT* sono vulnerabili alla manipolazione da parte di utenti malintenzionati. Questi possono sfruttare le debolezze del modello per ottenere risposte inappropriate o per ingannare altri utenti,

[152] Cfr. L. Califano, *Chat GPT e Meta EDI: spunti problematici su profili regolatori e ruolo delle autorità di controllo di protezione dati* in Federalismi.it, pubblicato il 3 maggio 2023, consultato il 16 maggio 2024.

aumentando il rischio di abusi e di informazioni fuorvianti. In sintesi, i *chatbot* basati su modelli di linguaggio come *GPT* offrono grandi potenzialità, ma è cruciale essere consapevoli anche dei possibili pericoli e lavorare costantemente per mitigare questi rischi attraverso un'adeguata supervisione e un miglioramento continuo dei sistemi di intelligenza artificiale[153].

2.4 **Il cloud computing: il comune denominatore dell'IoE**

Giunti a questo a paragrafo, come si è potuto notare sono due le cose che accomunano tutti gli ambiti di applicazione precedentemente descritti: la quantità enorme di dati in gioco e il *luogo* in cui immagazzinarli, ovvero la tecnologia di *cloud computing.*

La quantità di dati generata e utilizzata dai dispositivi *IoT* presenta una scelta fondamentale riguardo al sistema di elaborazione e conservazione dei dati. Si tratta di decidere tra una soluzione locale o una che sfrutta il *cloud computing*. Sebbene salvare i dati localmente possa sembrare più sicuro, le competenze informatiche di un consumatore medio difficilmente permetterebbero una gestione adeguata in autonomia. Pertanto, la scelta più comune è il *cloud*. Spesso questa scelta è anche inevitabile, poiché molti sistemi *IoT* raccolgono una tale quantità di dati che una soluzione locale diventa impraticabile, rendendo il *cloud* l'unica opzione. Inoltre, molti dispositivi *smart* domestici, come gli assistenti vocali, sono già predisposti per la conservazione dei dati nel *cloud*[154].

La diffusione dell'*IoT* sta rapidamente evolvendo, portandoci verso una realtà sempre più connessa. La vita quotidiana dell'uomo sarà sempre più integrata con sensori che collegano oggetti e persone, formando l'*Internet of Everything* (*IoE*). L'*IoE* mira a connettere tutto, fondendo il mondo fisico con quello virtuale, creando quella che Luciano Floridi ha chiamato *infosfera*[155].

Definire il *cloud* non è un compito semplice, ma un buon punto di partenza è affermare che il *cloud computing* non è una novità assoluta. Certamente, si tratta di

[153] Cfr. Di Tonto, *Intelligenza artificiale e nuovi diritti. Il caso chat gpt* cit.
[154] Cfr. Vizzoni, *Domotica e diritto. La Smart Home tra regole e responsablità* cit., pp. 18-19.
[155] Cfr. Vizzoni, *Domotica e diritto. La Smart Home tra regole e responsablità* cit., p. 16.

un'espressione e di una realtà commerciale nuova, ma in pratica abbraccia la vecchia idea del calcolo come servizio *utility*. Questa idea fu suggerita pubblicamente da John McCarthy nel 1961, il quale credeva che la potenza di calcolo sarebbe stata venduta tramite un modello di *business* basato sui servizi, come l'acqua o l'elettricità. Il problema era che le tecnologie *hardware*, *software* e di telecomunicazione non erano pronte ad accogliere questa innovazione. Tuttavia, una volta che i mezzi tecnologici si sono evoluti, la vecchia idea del calcolo come *utility* è ritornata con forza sotto il nome di *cloud computing*. Dietro il *cloud* ci sono molte tecnologie interdisciplinari, che rappresentano la ragione delle difficoltà nel definirlo chiaramente[156].

Il concetto di *cloud computing* richiama l'immagine di una nuvola, suggerendo l'idea di un insieme di dati, servizi e informazioni accessibili da qualsiasi luogo su richiesta. Sebbene spesso sia considerato come una metafora per l'etereo Internet, il *cloud computing* è in realtà un concetto più ampio e complesso, che include una vasta gamma di servizi al di là della semplice archiviazione dati. Questo concetto è stato descritto come un ecosistema di *networking* ubiquo e nuovo. Una delle definizioni più ampiamente accettate proviene dal *National Institute for Standards and Technology* (*NIST*), un'organizzazione americana che stabilisce standard di misurazione per lo sviluppo tecnologico industriale e commerciale. Secondo il NIST, il *cloud computing* è "*a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"*[157].

In parole semplici, il *cloud computing* si distingue per cinque elementi chiave: è un servizio disponibile su richiesta, accessibile da qualsiasi luogo tramite internet,

[156] Cfr. S. Cedrola, *GDPR in the cloud: who is who?* in Iusinitinere.it, pubblicato il 3.11.2019, consultato il 21.05.2024.

[157] Cfr. National Institute of Standards and Technology (NIST) *Definition of Cloud Computing, U.S. Department of Commerce*, Special Publication SP800-145, 2011, disponibile all'indirizzo http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, part. p. 2.

utilizza una risorsa centralizzata *pooling*, è scalabile e offre formule ottimizzate automaticamente per l'utente[158].

Oggi i servizi di *cloud computing* sono essenziali per lo svolgimento delle attività economiche, non solo per quelle tecnologicamente avanzate o *online*, ma anche per le attività tradizionali. Ad esempio, il *cloud* viene utilizzato per gestire la posta elettronica, *software* per ufficio, applicazioni finanziarie e contabili, archiviazione di file e *hosting* di *database*. Secondo il *National Institute of Standards and Technology* (*NIST*), il *cloud computing* è un'infrastruttura che, tramite internet, consente l'accesso online a un insieme condiviso di risorse come reti, *server* e servizi. Gli utenti possono utilizzare spazio di memorizzazione, *software* o ambienti di sviluppo senza che le risorse risiedano sui loro sistemi informatici, ma su *server* remoti gestiti da terze parti. Il *cloud computing* offre vantaggi significativi per le organizzazioni pubbliche e private, permettendo di adattare rapidamente i servizi alle esigenze del mercato, riducendo i costi e migliorando lo sviluppo di prodotti e servizi in un mercato in continua evoluzione. Inoltre, il *cloud computing* è cruciale per le politiche della Commissione Europea nel creare un mercato unico digitale europeo. I servizi di *cloud computing* sono disponibili attraverso diversi modelli di distribuzione, come classificato dal *NIST*. I principali modelli includono *Software as a Service* (SaaS), *Platform as a Service* (PaaS) e *Infrastructure as a Service* (IaaS). Il *SaaS* consente l'accesso remoto ad applicazioni e programmi *software*, il *PaaS* offre accesso al *layer* applicativo-esecutivo di una piattaforma *software* e strumenti per gestire dati, applicazioni e servizi, mentre l'*IaaS* fornisce accesso al sistema operativo tramite macchine virtuali e consente ai clienti di acquistare un ambiente *virtualizzato* e servizi di rete.

Le architetture di sistemi *cloud* possono essere private, pubbliche, ibride o di comunità. Un *cloud* privato è gestito interamente dall'organizzazione che lo utilizza e può essere fornito dai propri servizi IT o da terzi, mantenendo la sicurezza attraverso una rete privata. I *cloud* pubblici sono gestiti da un provider di servizi che condivide l'infrastruttura con diversi clienti tramite internet. Un *cloud* ibrido combina due o più

[158] Cfr. M. M. Winkler, J. Mosca, *Cloud computing e protezione dei dati personali* in Fumagalli Meraviglia M. (a cura di), *Diritto alla riservatezza e progresso tecnologico. Coesistenza pacifica e scontro di civiltà?*, I ed., Napoli, 2015, p. 123.

cloud di diverso tipo, mantenendoli distinti ma interconnessi, utile per organizzazioni con picchi di utilizzo occasionali. I *community cloud* sono offerti a un gruppo ristretto di organizzazioni con esigenze simili, e possono essere gestiti internamente o da un provider esterno. Il *cloud computing* è quindi un campo vasto e complesso, influenzato dalle dimensioni delle aziende di *cloud,* dalla tipologia di clientela (professionale o consumatori) e dai vari settori economici di utilizzo.[159]

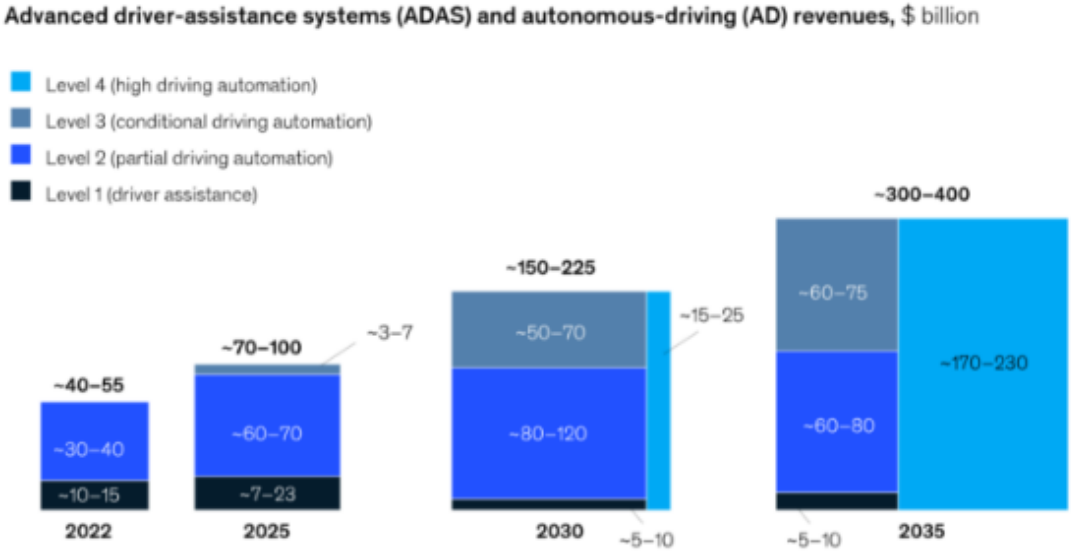
2.5 **Il volume economico di queste tecnologie**

Il mercato globale della domotica e dell'*Internet delle Cose* (*IoT*) continua a espandersi. Il controllo intelligente e remoto degli apparecchi e degli impianti connessi nelle abitazioni permette una significativa riduzione delle bollette domestiche, con una diminuzione del 20-25% dei consumi di gas ed elettricità, un calo del 5% dell'uso dell'acqua e circa un 30% in meno di sprechi alimentari. In attesa dell'operatività del *protocollo Matter*, che mira a garantire l'interoperabilità delle soluzioni di *smart home* grazie alla collaborazione delle principali aziende tecnologiche, le famiglie stanno adottando sempre più dispositivi connessi e comandi centralizzati, attivabili principalmente tramite comandi vocali o *contactless*. Secondo l'analisi dei trend di mercato condotta da *GFK Italia* per *Il Sole 24 Ore*, nel periodo gennaio-luglio 2023, rispetto agli stessi periodi del 2022 e del 2019 (pre-Covid), il settore ha registrato un aumento del 12% rispetto all'anno precedente e dell'84,5% rispetto al periodo pre-pandemia, favorendo gli elettrodomestici di massima efficienza e connessi. La ricerca annuale degli Osservatori Digital Innovation del Politecnico di Milano ha evidenziato che l'Italia è al primo posto in Europa per la crescita del mercato[160].

[159] Cfr. L. Valle, B. Russo, G. Bonzaghi, D. M. Locatello, *Struttura dei contratti e trattamento dei dati personali nei servizi di cloud computing alla luce del nuovo Reg. 2016/679 UE* in Contratto e Impresa/Europa, anno XXIII, pubblicazione annuale, 2018, p. 343-346.

[160] Cfr. P. Guidi, *Risparmio ed efficienza: è la corsa della domotica* in Il Sole 24 Ore, Milano, pubblicato il 23.09.2023, consultato il 20.05.2024.

Entro il 2035, la guida autonoma potrebbe generare tra i 300 e i 400 miliardi di dollari di entrate. Nuove ricerche evidenziano i requisiti necessari per emergere nel mercato in rapida evoluzione delle auto passeggeri. La visione di flotte di veicoli autonomi che trasportano persone in modo efficiente ha catturato l'immaginazione dei consumatori e stimolato ingenti investimenti negli ultimi anni. Nonostante alcuni ritardi che hanno posticipato il lancio dei veicoli autonomi ed il loro acquisto da parte dei clienti, la comunità della mobilità concorda ampiamente sul fatto che la guida autonoma possieda il potenziale per trasformare i trasporti, i comportamenti dei consumatori e la società nel suo complesso. Secondo una ricerca di McKinsey, la guida autonoma potrebbe creare un valore significativo per l'industria automobilistica, generando centinaia di miliardi di dollari entro la fine di questo decennio.



Diversi produttori stanno già sperimentando nuovi prodotti assicurativi, raccogliendo dati sui comportamenti di guida dalle tecnologie autonome e offrendo polizze personalizzate[161].

Il *business* della robotica è un fenomeno in crescita che va ben oltre la tecnologia, rappresentando un elemento chiave per l'*Industria 5.0* e la *Società 5.0*. I *robot*, sia collaborativi che di servizio, stanno diventando sempre più diffusi nei principali settori produttivi, consentendo di compensare la carenza di forza lavoro e il *gap* di

[161] Cfr. Mckinsey and Company, Autonomous driving's future: convenient and connected, pubblicato il 6.01.2023, consultato il 21.05.2024.

competenze previsto nei prossimi anni. Nel 2021 sono state prodotte 435.000 nuove unità robotiche, e si prevede che questo numero aumenterà a circa 518.000 unità annue entro il 2024. In particolare, i robot collaborativi sono passati da 19.000 a 22.000 unità tra il 2018 e il 2020, mentre i robot industriali tradizionali sono diminuiti da 404.000 a 362.000 unità. Geograficamente, l'Asia ha dominato il mercato con 266.000 nuove unità nel 2020, di cui 168.000 in Cina, seguita dall'Europa con 68.000 e dalle Americhe con 39.000 unità. La Corea del Sud ha la densità robotica più alta al mondo, con 932 robot ogni 10.000 lavoratori, seguita da Singapore (605), Giappone (390), Germania (371), Cina (246) e Italia (224). Nell'industria del tempo libero, il 53% delle realtà imprenditoriali utilizza la robotica, con l'83% che prevede di investire ulteriormente per migliorare la qualità delle esperienze e il coinvolgimento del pubblico. Nel *retail*, il 52% delle aziende utilizza la robotica per migliorare il *customer journey*, e il 73% prevede di aumentare gli investimenti[162].

Uno dei motivi per cui l'intelligenza artificiale è un tema così rilevante nelle agende di nazioni e comunità è la previsione che raggiungerà, in un tempo relativamente breve di cinque anni, un valore di 190,61 miliardi di dollari, con un tasso di crescita annuo del 36%. Anche in Italia l'interesse per l'IA è elevato; tuttavia, secondo i dati dell'Osservatorio Artificial Intelligence del Politecnico di Milano, solo il 12% delle imprese ha implementato almeno un progetto di intelligenza artificiale. Attualmente, metà delle aziende non ha ancora intrapreso iniziative, ma prevede di farlo: l'8% è in fase di implementazione, il 31% sta conducendo progetti pilota e il 21% ha stanziato budget per l'IA. Le applicazioni più comuni sono quelle dei *virtual assistant* e *chatbot*. Nonostante ciò, le imprese italiane hanno ancora una visione confusa delle opportunità offerte dall'intelligenza artificiale. L'espansione del mercato dei sistemi di IA, con tutte le sue implicazioni, comporta conseguenze economiche, etiche e socio-antropologiche che influenzano anche il settore della giustizia penale[163].

---

[162] Cfr. F. La Trofa, *Il business della robotica: prospettive e analisi di mercato* in Tech4future, pubblicato il 24-06.2022, consultato il 21.05.2024.

[163] Cfr. C. Limiti, *Intelligenza artificiale: implicazioni etiche in termini in materia di privacy e diritto penale* in Iusinitinere.it, pubblicato il 9.02.2021, consultato il 21.05.2024.

Il rapporto della società di consulenza americana McKinsey rivela un dato di notevole rilevanza: l'intelligenza artificiale generativa (*GenAI*) potrebbe contribuire all'economia globale con una cifra compresa tra 2,6 e 4,4 trilioni di dollari all'anno, equivalente al prodotto interno lordo del Regno Unito, che nel 2021 si è attestato a 3,1 trilioni di dollari. Rispetto alle stime precedenti della stessa McKinsey, l'impatto economico degli algoritmi è significativamente aumentato, passando dal 15% previsto nel 2017 al 40% della valutazione più recente. Gli analisti attribuiscono questa accelerazione alla rapidità con cui strumenti come *ChatGPT*, *Bing* di *Microsoft*, *Bard* di *Google* e *Ernie* di *Baidu* sono stati adottati dal pubblico e alla vasta gamma di applicazioni potenziali nel contesto aziendale, comprese le piccole imprese. Gli esperti prevedono che gran parte del valore economico derivante dalla *GenAI* sarà legato all'automazione delle attività di gestione dei clienti (circa la metà dei contatti con i clienti nel settore bancario e delle telecomunicazioni in Nord America è già gestita da bot e sistemi automatizzati), ai processi di *marketing* e vendita, e all'incremento della produttività nel campo dell'ingegneria del *software* (per la generazione di bozze di codice, correzione e *refactoring* del codice stesso) e della ricerca e sviluppo, dove l'AI generativa aiuterà progettisti e *designer* a ridurre i costi selezionando e utilizzando i materiali in modo più efficiente.

In generale, McKinsey considera l'innovazione algoritmica come un *catalizzatore tecnologico* capace di spingere le industrie verso l'automazione e di liberare il potenziale creativo dei lavoratori. Questo progresso tecnologico richiederà una leadership rafforzata nel settore tecnologico, inclusi interventi delle autorità di regolamentazione[164].

Il mercato dell'Intelligenza Artificiale in Italia ha registrato una crescita significativa nel 2023, aumentando del 52% e raggiungendo un valore di 760 milioni di euro. La progressione di sviluppo è stata la seguente: +24% nel 2019, +15% nel 2020, +27% nel 2021, +32% nel 2022, e infine +52% nell'ultimo anno, determinando una crescita complessiva del mercato del 262% negli ultimi cinque anni. La maggior parte degli investimenti è destinata a soluzioni di analisi e interpretazione dei testi

[164] Cfr. G. Rusconi, *Quanto vale l'intelligenza artificiale generativa? Impatto potenziale da 4,4 migliaia di miliardi di dollari* in Il Sole 24 ore, pubblicato il 24.06.2023, consultato il 20.05.2024.

per ricerca semantica, classificazione, sintesi e spiegazione di documenti o agenti conversazionali tradizionali. Tuttavia, i progetti di intelligenza artificiale generativa rappresentano ancora solo il 5% del totale degli investimenti, con un valore di 38 milioni di euro. Sei grandi imprese italiane su dieci hanno già intrapreso progetti di intelligenza artificiale, almeno a livello sperimentale, e due su tre hanno discusso internamente delle applicazioni dell'IA Generativa, con una su quattro che ha avviato una sperimentazione (17% del totale)[165].

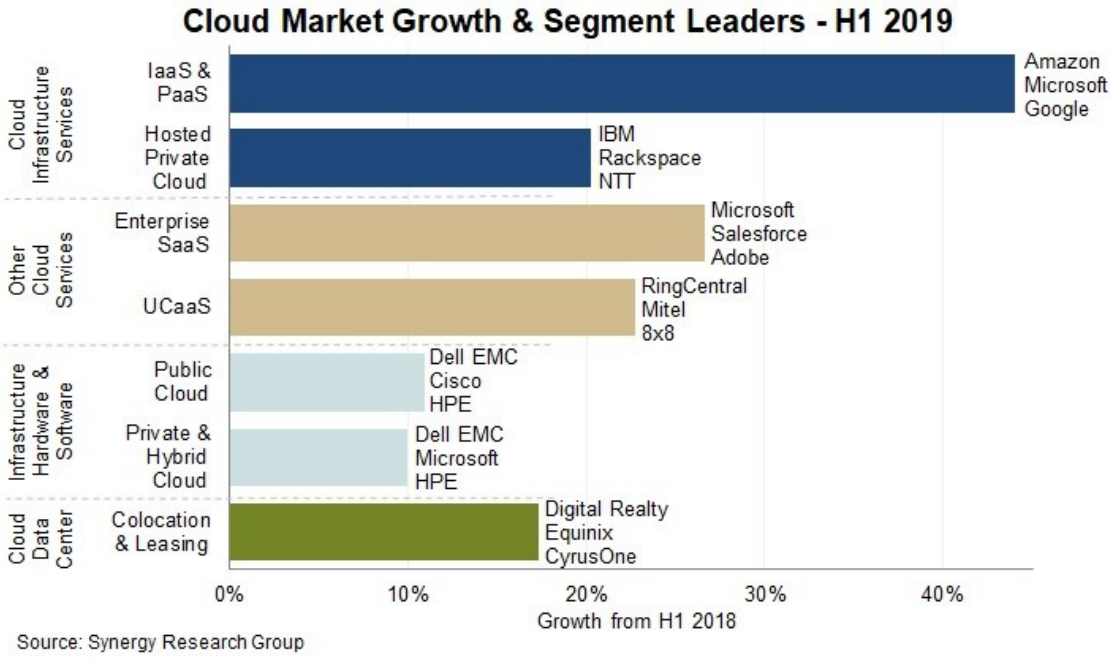
I dati recenti del *Synergy Research Group* mostrano che, nei primi sei mesi del 2019, i ricavi degli operatori e dei fornitori nei sette segmenti chiave del mercato dei servizi *cloud* e delle infrastrutture hanno superato i 150 miliardi di dollari, con una crescita del 24% rispetto al primo semestre del 2018. Nei segmenti dei servizi *cloud*, *IaaS* e *PaaS* hanno registrato il tasso di crescita più elevato, pari al 44%, seguiti da *SaaS* aziendale con il 27%, *UCaaS* con il 23% e i servizi di infrastruttura *cloud* privata ospitata con il 20%. La spesa per *hardware* e *software* per infrastrutture pubbliche, private e ibride è cresciuta di poco oltre il 10%, mentre la spesa dei fornitori di *cloud* per servizi di *colocation* e *leasing* di *data center* è aumentata del 17%.

[165] Cfr. S. Casini, *Intelligenza artificiale, crescita record del mercato in Italia (+52%): in 10 anni sostituirà il lavoro di circa 3,8 milioni di persone* in Innovation Post, pubblicato il 1.02.2024, consultato il 22.05.2024.

Complessivamente, la spesa per i servizi *cloud* supera ora di gran lunga quella per le infrastrutture di *data center* di supporto. Le aziende che si sono distinte maggiormente nei vari segmenti di mercato nel primo semestre del 2019 sono *Microsoft*, *Amazon*/*AWS*, *Dell EMC*, *Cisco*, *HPE* e *Google*. Altri attori rilevanti includono *Salesforce*, *Adobe*, *VMware*, *IBM*, *Digital Realty*, *Equinix* e *Rackspace*. Complessivamente, queste aziende rappresentano oltre la metà di tutti i ricavi legati al *cloud*. Nel primo semestre del 2019, la spesa totale per hardware e software utilizzati per costruire infrastrutture *cloud* ha raggiunto quasi 55 miliardi di dollari, suddivisi in modo abbastanza uniforme tra *cloud* pubblici e privati. Gli investimenti infrastrutturali dei fornitori di servizi *cloud* hanno permesso loro di generare oltre 90 miliardi di dollari di ricavi dai servizi di infrastruttura *cloud* (*IaaS*, *PaaS*, servizi di *cloud* privato ospitato) e dal *SaaS* aziendale, oltre a supportare servizi *internet* come ricerca, *social networking*, *email*, *e-commerce*, *gaming* e *app* mobili. Questi fornitori di *cloud* necessitano di spazi per ospitare le loro infrastrutture, quindi la spesa per il *leasing* di *data center* e i servizi di *colocation* continua a crescere fortemente. Nel frattempo, *UCaaS*, sebbene rappresenti un mercato di tipo diverso, sta crescendo rapidamente e sta apportando cambiamenti radicali nelle comunicazioni aziendali.

"Il mercato associato al *cloud* sta crescendo a tassi che vanno dal 10% a oltre il 40%, e la spesa annuale per il cloud raddoppierà in meno di quattro anni. Il *cloud* sta dominando sempre di più il panorama IT", ha affermato John Dinsdale, capo analista presso *Synergy Research Group*. "Il *cloud* ha aperto una gamma di opportunità per nuovi entranti nel mercato e per tecnologie e modelli di business dirompenti. *Amazon* e *Microsoft* hanno guidato il cambiamento e la crescita aggressiva delle entrate del *cloud*, ma molte altre aziende tecnologiche ne stanno beneficiando. Il rovescio della medaglia è che alcuni attori tradizionali dell'IT stanno avendo difficoltà a bilanciare la protezione delle attività legacy con la necessità di abbracciare pienamente il *cloud*"[166].

[166] Cfr. Synergy Research group*, Half-Yearly Review Shows $150 billion Spent on Cloud Services and Infrastructure*, Reno, pubblicato il 19.09.2019, consultato il 22.05.2024.


Cloud Market Growth & Segment Leaders - H1 2019
Cloud Infrastructure Services
IaaS & PaaS
Amazon
Microsoft
Google
Hosted Private Cloud
IBM
Rackspace
NTT
Other Cloud Services
Enterprise SaaS
Microsoft
Salesforce
Adobe
UCaaS
RingCentral
Mitel
8x8
Infrastructure Hardware & Software
Public Cloud
Dell EMC
Cisco
HPE
Private & Hybrid Cloud
Dell EMC
Microsoft
HPE
Cloud Data Center
Colocation & Leasing
Digital Realty
Equinix
CyrusOne
0%
10%
20%
30%
40%
Growth from H1 2018
Source: Synergy Research Group

Capitolo 3
IMPLICAZIONI DI TALI TECNOLOGIE COL GDPR: FOCUS SUI SOGGETTI DEL TRATTAMENTO

Prima di addentrarsi nei profili critici derivanti dall'interazione tra tecnologie e GDPR, è ritenuto utile esplicare una problematica di ordine generale derivante dall'utilizzo dei *Big Data*, che si va ad aggiungere a quelle seguenti.

Il Regolamento 2016/679 sembra non riuscire a superare la sfida posta dai *Big Data*. Questo non significa che esso non offra spunti utili per risolvere le problematiche legate alla nuova gestione delle informazioni, ma, come evidenziato da Mayer-Schönberger, rappresenta solo un punto di partenza. In particolare, il legislatore europeo non è riuscito a prevedere l'impatto delle applicazioni tecnologiche che avrebbero dovuto caratterizzare l'orizzonte ventennale annunciato. Il Regolamento non ha apportato innovazioni radicali ai principi che, dagli anni '90, hanno sostenuto il quadro normativo comunitario in materia. Tuttavia, l'ultimo decennio del secolo scorso è completamente diverso dal contesto attuale, dal punto di vista socio-tecnologico. Basti pensare che nel 1995, anno in cui fu approvata la Direttiva 95/46/CE, solo lo 0,5% della popolazione italiana utilizzava *Internet*, *Google* e *Facebook* non esistevano e uno dei *computer* più potenti al mondo (l'*ASCI Red*) aveva appena superato la soglia di 1 *teraflop* di capacità di calcolo.

Questo approccio conservativo del legislatore europeo fa sì che l'intento di regolamentare efficacemente i *Big Data* si scontri con tre diversi tipi di ostacoli: un'interpretazione restrittiva del principio di finalità del trattamento, l'incertezza dell'autodeterminazione individuale nel contesto dei *Big Data* e la mancata considerazione dell'impatto collettivo dell'uso dei dati a scapito di una visione più ampia[167].

[167] Cfr. A. Mantelero, *La privacy all'epoca dei Big Data* in V. Cuffaro, R. Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, I ed., Torino, 2019, p. 1182.

Questo approccio, che si basa su tendenze e correlazioni presunte tra i dati, comporta una modalità diversa di progettare l'indagine sociale. Invece di partire da ipotesi di ricerca specifiche e predefinite, sono i dati stessi e il loro dinamismo a suggerire possibili relazioni tra fatti e comportamenti. In questo modo, l'analisi dei dati permette di individuare gli aspetti specifici meritevoli di approfondimento, che poi possono essere esaminati con metodi tradizionali. Con questo approccio, al momento della raccolta dei dati, è possibile formulare solo ipotesi di ricerca molto generali, poiché le inferenze potenziali derivanti dai dati sono ancora sconosciute. Lo scopo specifico del trattamento dei dati potrà quindi essere identificato solo successivamente, quando l'analisi iniziale metterà in luce l'utilità di specifiche informazioni per rivelare determinati aspetti. Questi aspetti potranno poi essere verificati e analizzati mediante l'uso di metodi statistici tradizionali[168].

Un'ulteriore preoccupazione riguarda i *bias* introdotti attraverso i dati utilizzati per addestrare i *computer* a comprendere e prevedere il mondo con cui interagiscono. Poiché le macchine apprendono dalle informazioni fornite loro e non hanno modo di verificare queste informazioni con un contesto più ampio, qualsiasi pregiudizio presente nel *set* di dati iniziale influenzerà le previsioni fatte. Se queste previsioni vengono utilizzate per prendere decisioni, si crea un circolo vizioso in cui il *feedback* che la macchina riceve rafforza il pregiudizio iniziale. Il quadro normativo sulla protezione dei dati in Europa richiede alle organizzazioni (titolari del trattamento) di essere trasparenti riguardo agli algoritmi che utilizzano. Questo è particolarmente complesso nel campo del *machine learning*, dove gli algoritmi possono essere sconosciuti e imprevedibili persino per gli sviluppatori di sistemi di IA, dato che come già detto nello scorso capitolo, la progettazione degli algoritmi è parte integrante del processo di apprendimento automatico stesso[169].

Nel complesso, sia i *big data analytics* che individuano tendenze e correlazioni, sia quelli basati su algoritmi di *machine learning*, sollevano criticità nel tradizionale modello di tutela dei dati personali, che si basa sull'autodeterminazione individuale riguardo alle informazioni personali. In molti casi, infatti, le finalità o le modalità del

[168] Cfr. Mantelero, *La privacy all'epoca dei Big Data* cit., p. 1188.
[169] Cfr. G. Buttarelli, *A smart approach: counteract the bias in artificial intelligence*, in www.edps.europa.eu, 8.11.2016, consultato il 29.05.2024.

trattamento dei dati sono solo parzialmente conosciute, facendo venire meno uno degli elementi essenziali che consentono agli individui di valutare le conseguenze delle proprie decisioni. Inoltre, nel contesto dei *big data*, la complessità dell'elaborazione dei dati accentua ulteriormente i già noti limiti dell'effettiva autodeterminazione individuale nel trattamento dei dati, che caratterizzano il modello del consenso informato in generale. In termini di informativa, la complessità dei processi e la difficoltà nel definire chiaramente i possibili utilizzi dei dati portano a creare informative che risultano generiche e vaghe riguardo alle finalità, oppure estremamente dettagliate e tecniche[170].

Nello scenario dei *big data*, l'analisi delle informazioni si concentra sempre meno sul singolo individuo e sulla sua identificazione specifica, privilegiando invece lo studio su larga scala di gruppi di persone, a volte molto ampi, che possono coinvolgere milioni di individui. L'obiettivo della raccolta e dell'analisi dei dati è sempre più orientato a studiare il comportamento di questi gruppi e a prevederne i futuri sviluppi, piuttosto che a profilare il singolo. Di conseguenza, gli individui sono considerati in base alla loro appartenenza a un gruppo specifico (si pensi, ad esempio, alle tecniche di discriminazione dei prezzi). In questo contesto, sia nel settore commerciale che in quello della pubblica amministrazione (ad esempio, nelle politiche sociali o nella prevenzione del crimine), si tende a definire strategie generali su vasta scala, elaborate a partire da rappresentazioni della società generate da algoritmi predittivi. Queste strategie vengono poi applicate agli individui identificati in base alla loro appartenenza a uno o più gruppi delineati dagli *analytics*.

Questo approccio basato su categorie di appartenenza porta i decisori ad adottare soluzioni comuni per tutti gli individui classificati all'interno dello stesso gruppo creato dagli *analytics*. In tal modo, l'uso dei dati trascende la dimensione individuale e assume una dimensione collettiva, con potenziali implicazioni pregiudizievoli per i soggetti coinvolti[171].

[170] Cfr. Mantelero, *La privacy all'epoca dei Big Data* cit., p. 1189.
[171] Cfr. Mantelero, *La privacy all'epoca dei Big Data* cit., pp. 1196 s.

3.1 **Cloud computing e titolare del trattamento**

Il funzionamento generale del sistema è garantito dai diversi ruoli degli "*attori*" del *cloud computing*. I quali si dividono in: *cloud provider*, ossia i proprietari e gestori dei servizi di *cloud computing*; *cloud customer*, ovvero coloro che incaricano i provider per la creazione di tali servizi; e infine i *cloud user*, i clienti che utilizzano questi servizi. All'interno della struttura del *cloud*, ciascun soggetto ha un ruolo specifico e distinto dagli altri. Per quanto riguarda le varie tipologie di servizi offerti dal *cloud*, in uno schema verticistico, possiamo affermare che man mano che si scende, diminuisce il controllo esercitato dal fornitore del servizio *cloud*, mentre aumenta il potere dell'utente finale. Ad esempio, nel caso del *SaaS* – come nel caso di *Facebook* – il fornitore del servizio ha un alto grado di autonomia e può determinare quasi esclusivamente il destino delle informazioni depositate dall'utente. Questo rischio è inferiore, anche se ancora presente, nel caso del *PaaS* e del *IaaS*, dove l'utente è comunque vincolato agli standard di archiviazione delle informazioni dei singoli fornitori a cui si rivolge (noto come *lock-in*)[172].

Nei rapporti contrattuali di *cloud computing* è tipico che il *CSP* e l'utente finale non siano gli unici attori coinvolti nell'erogazione del servizio. Spesso, infatti, il *CSP* ricorre a terzi *subproviders* per erogare parte del servizio. Ad esempio, una piccola società di sviluppo *software* può fornire un proprio programma in modalità *SaaS* e, allo stesso tempo, affidare a un terzo *CSP* il servizio di *storage*, utilizzando un fornitore di servizi *IaaS*. Analogamente, un *CSP* che fornisce *IaaS* può utilizzare servizi di sicurezza software offerti da un *CSP SaaS*.

I giganti del settore *ICT* ricorrono spesso al *subcontracting*. Una ricerca sui *Terms of Service* di quattro dei principali fornitori di servizi *PaaS* e *IaaS* ha rivelato che questi includono sempre una clausola che permette al *CSP* di avvalersi di terze parti "*for processing purpose*". Il *subprovider* può essere un colosso del settore informatico, che offre *spazio* a costi relativamente bassi nei propri *data center* sparsi sul pianeta, o una piccola azienda che fornisce un servizio specifico incluso nel pacchetto offerto dal *CSP* al cliente. Spesso, il *subcontractor* stipula ulteriori

[172] Cfr. M. M. Winkler, J. Mosca, *Cloud computing e protezione dei dati personali* in Fumagalli Meraviglia M. (a cura di), *Diritto alla riservatezza e progresso tecnologico. Coesistenza pacifica e scontro di civiltà?*, I ed., Napoli, 2015, p. 127.

subcontratti, creando una complessa catena di fornitori. Questa catena non è inflessibile e statica, ma altamente dinamica. Durante la fornitura del servizio, il *CSP* può modificare uno o più collaboratori, come indicato nei *Terms of Service*, per assicurarsi lo stesso servizio a costi ridotti, inserendo o togliendo collaboratori per esternalizzare ulteriormente una parte del servizio fornito all'utente finale o per fornire direttamente parte del servizio[173].

L'effettivo ruolo dei soggetti coinvolti nei servizi di *cloud computing* dev'essere ora coordinato con il Regolamento 2016/679. La determinazione delle posizioni del *Cloud Service Provider* (*CSP*), del cliente e dei subfornitori come titolari o responsabili del trattamento dei dati personali individua le attività e le responsabilità a cui sono tenuti nel trattamento dei dati personali nei servizi *cloud*. L'importanza di definire chiaramente i ruoli dei soggetti coinvolti è evidente, poiché nel trattamento dei dati nelle operazioni di *big data* e *cloud computing*, il rapporto tra titolare e responsabile, o subfornitori, è diventato sempre più complesso. Questo è dovuto al fatto che, sotto la normativa precedente al nuovo Regolamento, i responsabili tendevano a ottenere un maggiore controllo reale senza incorrere in responsabilità e le due figure potevano trovarsi in Stati diversi, creando problemi nella regolamentazione del trasferimento dei dati[174].

È importante notare che la normativa comunitaria sui dati personali è strutturata in modo dato-centrico. Ciò significa che il ruolo di chi tratta i dati è determinato dalla relazione legittima che ciascuno instaura coi dati, piuttosto che dall'origine dei rapporti tra le parti. Di conseguenza, l'organizzazione del trattamento dei dati, basata su una tripartizione sostanziale delle figure coinvolte, non coincide necessariamente con la struttura aziendale né è influenzata dall'autonomia delle parti contraenti[175].

In linea teorica, si può qualificare il flusso di dati generato dall'erogazione del servizio di *cloud computing* come un flusso tra due titolari autonomi o tra un titolare

---

[173] Cfr. L. Valle, B. Russo, G. Bonzaghi, D. M. Locatello, *Struttura dei contratti e trattamento dei dati personali nei servizi di cloud computing alla luce del nuovo Reg. 2016/679 UE* in Contratto e Impresa/Europa, anno XXIII, pubblicazione annuale, 2018, pp. 364-365.

[174] Cfr. Valle, Russo, Bonzaghi, Locatello, *Struttura dei contratti e trattamento dei dati personali nei servizi di cloud computing alla luce del nuovo Reg. 2016/679 UE* cit., p. 370.

[175] Cfr. A. Mantelero, *Processi di outsourcing informatico e cloud computing: la gestione dei dati personali ed aziendali* in Diritto dell'informazione e dell'informatica, anno XXVI, n. 4-5, 2010, p. 679.

e un responsabile. Nel primo caso, poiché ogni parte tratta i dati in modo autonomo, il fruitore dei servizi *cloud* non sarà responsabile per eventuali illeciti commessi dal *cloud provider* nel trattamento dei dati. Al contrario, se il fornitore del servizio *cloud* è considerato un titolare autonomo, il fruitore perde la capacità di dirigere il trattamento dei dati effettuato attraverso il servizio. Invece, se si considera il rapporto tra il fruitore del servizio *cloud* come titolare e il fornitore del *cloud* come responsabile, il fruitore avrà un maggiore controllo sulla gestione dei dati. Tuttavia, ciò comporterà anche la responsabilità per gli aspetti organizzativi e di sicurezza della gestione dei dati effettuata dal fornitore, oltre alla responsabilità di scegliere un fornitore affidabile e competente, come richiesto dall'art. 28, paragrafo 1, del Regolamento[176].

La classificazione del ruolo del *Cloud Service Provider* (*CSP*) come titolare o responsabile del trattamento dei dati personali è in discussione da tempo. Fino ad ora, il parere prevalente ha individuato il *CSP* come responsabile. Questo ruolo di responsabile del trattamento, e non di titolare, è principalmente congiunto all'origine delle attività svolte dal *CSP*, specificamente come fornitore di *cloud storage*. Il *cloud provider* gestisce servizi che offrono sistemi di conservazione e archiviazione dei dati per conto del cliente, rendendoli immediatamente disponibili a chiunque abbia l'autorizzazione all'accesso, in qualsiasi parte del mondo e a qualsiasi ora, attraverso una connessione *internet*.

Già nel 2010, il Gruppo Articolo 29 aveva prospettato la qualifica di responsabile per i fornitori di servizi di *hosting* su *internet*, ossia per tutti quegli operatori che rendevano fruibili le proprie infrastrutture per la conservazione dei dati altrui. Questi erano i precursori degli operatori *cloud*, che lo stesso organismo europeo riconosceva come possibili nuove frontiere del concetto di responsabile. L'opinione del WP 196 del 2012 confermava questo pensiero, specificando che il fornitore *cloud* è equiparato alla figura del responsabile del trattamento. Il *cloud provider* era identificato esclusivamente come responsabile, che agisce come se fosse

[176] Cfr. A. Mantelero, *Il cloud computing* in R. Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato: commentario al regolamento UE n.2016/79 (GDPR) e al novellato D. Lgs n. 196/2003 (Codice Privacy): scritti in memoria di Stefano Rodotà*, I ed., Milano, 2019, pp. 519-520.

un'estensione del cliente, il quale rimane l'unico titolare del trattamento dei dati salvati e conservati nei *server* del *cloud provider*. Si escludeva espressamente ogni identificazione del *provider* con la figura del titolare, poiché la decisione finale sul trattamento dei dati rimane sempre al cliente. Quest'ultimo, nonostante a volte avesse un potere contrattuale limitato, aveva sempre la possibilità di rifiutare i contratti proposti dal *cloud provider*[177].

Considerando i criteri indicati e le situazioni concrete in cui si svolgono i processi informatici in modalità *cloud*, è importante esaminare vari elementi per definire il ruolo delle parti coinvolte. Nei seguenti contesti, il cliente, in qualità di titolare, affida il trattamento dei dati al fornitore del servizio, che agisce come responsabile.

Il cliente ha l'autorizzazione degli interessati a trattare i dati, mentre i terzi, come il fornitore del servizio *cloud*, possono gestire le informazioni solo nell'interesse del cliente. Il fornitore del servizio, pur avendo un certo margine di autonomia decisionale e operativa, deve rispettare compiti "chiaramente e rigorosamente definiti". Le prestazioni del fornitore sono regolate contrattualmente, spesso tramite un *Service Level Agreement* (*SLA*) e dei *Key Performance Indicators* (*KPI*). Il cliente decide le finalità e le modalità di utilizzo del *software* per il trattamento dei dati, mentre il fornitore gestisce solo una parte di questi trattamenti. Infine, il fornitore del servizio non ha una competenza professionale esclusiva e predominante che gli conferisca un alto grado di autonomia. Piuttosto, deve garantire un elevato *standard* tecnico-qualitativo nell'erogazione di servizi che prima erano gestiti internamente all'azienda[178].

Pertanto, spetta al cliente effettuare la valutazione d'impatto sulla protezione dei dati che intende trattare e, se necessario, dotarsi di un responsabile della protezione dei dati. Tuttavia, è importante chiarire che il cliente può delegare al fornitore *cloud* la scelta delle misure tecniche e organizzative da adottare per raggiungere gli obiettivi del titolare, rendendo così il fornitore responsabile. Di conseguenza, il dovere principale del cliente è selezionare un fornitore *cloud* che garantisca il rispetto della normativa sulla protezione dei dati, applicando il principio di

[177] Cfr. Valle, Russo, Bonzaghi, Locatello, *Struttura dei contratti e trattamento dei dati personali nei servizi di cloud computing alla luce del nuovo Reg. 2016/679 UE* cit., pp. 370-371.
[178] Cfr. Mantelero, *Il Colud Computing* cit., pp. 520-521.

adeguatezza previsto dall'art. 28.1, che richiede di scegliere responsabili che offrano sufficienti garanzie per implementare misure tecniche e organizzative adeguate a garantire la conformità e la protezione dei diritti degli interessati.

Inoltre, considerato che il *cloud computing* rappresenta un settore di servizi complessi basato su tecnologie multilivello, l'*accountability* assume una connotazione particolare. Sia il cliente *cloud* che i fornitori (e i subcontraenti) possono avere diversi gradi di responsabilità. Ad esempio, anche se il titolare è inizialmente responsabile del trattamento dei dati, in caso di violazione dei dati sulla piattaforma *cloud*, il fornitore sarà il principale responsabile della gestione dei problemi di sicurezza e della notifica all'autorità o agli interessati, informando il cliente come previsto dall'art. 33.2. Il fornitore, come fornitore della tecnologia, dovrebbe adottare tutte le misure tecniche e organizzative necessarie per attuare i principi di protezione dei dati e fornire documentazione che dimostri la loro implementazione. Ad esempio, il fornitore deve implementare procedure per rispondere alle richieste di accesso e applicare i principi di protezione dei dati *by-design* e *by-default*, ottenere certificazioni, effettuare la *DPIA*, come previsto dall'art. 28.1.

Di conseguenza, anche se il cliente è il titolare, il fornitore, in quanto responsabile, deve adempiere a una serie di obblighi che permettano all'autorità di effettuare controlli e al cliente di conoscere gli aspetti dell'organizzazione e della sicurezza del fornitore, per scegliere un fornitore *cloud* che garantisca il rispetto della normativa sulla protezione dei dati. L'applicazione del GDPR, che esplicita i principi degli artt. 24 e 25, facilita questa scelta grazie ai meccanismi di certificazione che garantiscono la conformità normativa da parte dei responsabili, limitando l'intervento di numerosi terzi indipendenti che potrebbero compromettere la sicurezza del *cloud provider*.

Inoltre, in relazione alla gestione delle richieste per l'esercizio dei diritti degli interessati ex art. 28.2.e), il modello del *cloud* può essere esemplare. Anche se il fornitore agisce come responsabile, essendo il produttore della tecnologia che supporta il servizio del cliente, è suo compito implementare procedure per rispondere alle richieste di accesso o rettifica in modo elettronico e/o automatizzato. Quindi, anche se la responsabilità iniziale ricade sul titolare, il responsabile, che è anche

produttore dei servizi o applicazioni, deve adempiere a crescenti obblighi proporzionalmente alle funzioni delegate, considerando la natura, le finalità del trattamento, il tipo di dati personali e le categorie di interessati[179].

È stato da tempo sottolineato che qualificare il *CSP* come responsabile del trattamento non può essere fatto in modo assoluto. Un primo problema si presentava quando sia il cliente sia il *CSP* avevano una significativa libertà decisionale sulle scelte fondamentali del trattamento dei dati: in questo caso, il cliente e il *provider* erano considerati come due distinti titolari, con la conseguenza che lo scambio di dati tra loro configurava una trasmissione di dati. Con l'avvento del GDPR, questo problema sembra risolto grazie all'introduzione del concetto di contitolari riferito ai due soggetti. Le situazioni in cui il *cloud provider*, pur non essendo formalmente titolare del trattamento dei dati, mostrava comportamenti che lo qualificavano di fatto come titolare e non come responsabile, venivano risolte in passato valutando solo il potere decisionale sul trattamento, indipendentemente da eventuali vincoli contrattuali. Questo approccio è confermato dal GDPR, che definisce il titolare del trattamento come colui che determina le finalità e i mezzi del trattamento dei dati personali (art. 4, par. 7 GDPR). Secondo l'autore, con la nuova normativa sarà più probabile che il *cloud provider*, formalmente indicato come responsabile, venga riqualificato come contitolare piuttosto che come unico titolare. Il nuovo Regolamento impone al cliente (art. 28, par. 1) di scegliere il proprio responsabile tra coloro che garantiscono un adeguato livello di protezione dei dati. Pertanto, diventa difficile sostenere una completa estraneità del cliente nelle scelte relative al trattamento dei dati, condizione necessaria per negare totalmente la responsabilità come titolare. Come correttamente ricordato, l'obbligo di un contratto scritto, anche in forma elettronica, può aiutare a meglio individuare poteri decisionali e responsabilità.

In generale, nei processi di esternalizzazione dei servizi informatici in ambito aziendale, l'impresa che utilizza il servizio *cloud* può essere considerata come *controller*, mentre il fornitore del servizio assume il ruolo di *processor*. Questa

[179] Cfr. L. Bolognini, E. Pelino, C. Bistolfi, *Le obbligazioni di compliance in materia di protezione dei dati* in L. Bolognini, E. Pelino, C. Bistolfi, *Il regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali,* I ed., Milano, 2016, pp. 338 s.

distinzione ha carattere generale e può variare in base alle specifiche circostanze del rapporto tra le parti del contratto di *cloud computing* e i dati, specialmente riguardo alla contitolarità. L'art. 26 del Regolamento, basandosi sul lavoro del Gruppo di Lavoro Articolo 29 per la protezione dei dati, definisce la contitolarità come la situazione in cui "*due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento*". In questi casi, i contratti *cloud* devono includere un accordo che definisca le responsabilità delle parti in merito agli obblighi derivanti dal Regolamento, in particolare riguardo all'esercizio dei diritti dell'interessato e all'informativa, a meno che una norma di legge non stabilisca tali responsabilità[180].

La norma prevede inoltre che questa parte dell'accordo sia resa pubblica, almeno nei suoi "contenuti essenziali", a favore degli interessati, i quali possono comunque esercitare i propri diritti nei confronti di ciascun titolare del trattamento. Quando si utilizza il *cloud* per fornire servizi a una generica utenza *consumer*, il trattamento che costituisce il servizio erogato (come posta elettronica o *social network*) prevale su quello di esternalizzazione dei processi informatici. Anche nei modelli di *software as a service*, in questi casi, il fornitore del servizio *cloud* assume il ruolo di titolare del trattamento[181].

Si è precedentemente trattato della possibilità che vengano utilizzati dei *subproviders*. Risulta più difficile l'analisi dei problemi giuridici legati al trattamento e alla protezione dei dati personali nel *cloud*, soprattutto alla luce delle novità introdotte dal Regolamento 2016/679. Come già evidenziato, nel caso in cui il *cloud customer* sia un'impresa o un professionista che utilizza la tecnologia *cloud* per gestire alcuni aspetti della propria attività, come la contabilità, i rapporti di lavoro o l'archiviazione di atti e documenti contenenti dati sensibili dei clienti, il *CSP* assume il ruolo di mero *data processor*. Di conseguenza, i *subproviders* ai quali il *CSP* fa riferimento per l'erogazione di parte del servizio, e che hanno il permesso di trattare (accedere o semplicemente conservare) i dati personali raccolti e trattati dal *cloud customer* in qualità di titolare, devono essere considerati come *another processor* (o

[180] Cfr. L. Valle, B. Russo, D. M. Locatello, G. Bonzaghi, *Privacy e contratti di Cloud Computing* in E. Tosi (a cura di), *Privacy Digital. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy,* I ed., Milano, 2019, pp. 522-523.

[181] Cfr. Mantelero, *Il Cloud Computing* cit., pp. 521-522.

subprocessor) secondo quanto stabilito dall'art. 28 GDPR, che disciplina i rapporti tra i vari soggetti coinvolti nel trattamento.

L'esistenza della rete dei *subprocessors* implica numerosi rischi per la sicurezza dei dati personali nel *cloud*. È frequente che i dati siano trattati da *subprocessors* la cui identità e localizzazione geografica sono sconosciute all'utente finale. Questo comporta per quest'ultimo, che è regolarmente *data controller*, una significativa diminuzione del controllo sui dati immessi nel *cloud*. I dati potrebbero diventare temporaneamente o permanentemente inaccessibili per diverse ragioni legate ai *subcontractors* o essere esposti all'accesso di terzi non autorizzati (*data breaches*), ancora una volta all'insaputa del *cloud customer*[182].

Il titolare ha il diritto di opporsi a eventuali aggiunte o sostituzioni dei responsabili designati, e il responsabile del trattamento deve informarlo in tal senso. I fornitori di servizi *cloud* possono quindi includere clausole nei contratti per ottenere dai titolari l'autorizzazione a nominare terze parti nella loro filiera. È importante notare che i sub-responsabili saranno soggetti agli stessi obblighi del responsabile iniziale nominato dal titolare. Infatti, ai sensi dell'art. 28, par. 4 del Regolamento, quando un responsabile del trattamento delega a un altro responsabile specifiche attività di trattamento per conto del titolare, a quest'ultimo sono imposti, tramite contratto o altro atto giuridico conforme al diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati previsti nel contratto tra il titolare e il responsabile iniziale.

Questo accordo deve includere garanzie specifiche che assicurino l'adozione di misure tecniche e organizzative adeguate per conformarsi al Regolamento. Inoltre, il primo responsabile del trattamento rimane solidalmente responsabile verso il titolare nel caso in cui il sub-responsabile non rispetti i propri obblighi di protezione dei dati. Nonostante questa impostazione normativa semplifichi formalmente la nomina dei sub-responsabili, rimane il problema che il titolare spesso non ha la capacità di valutare l'idoneità dei terzi nominati dal responsabile per svolgere le attività assegnate. Questo rende difficile rispettare il principio di *accountability* previsto

[182] Cfr. Valle, Russo, Bonzaghi, Locatello, *Struttura dei contratti e trattamento dei dati personali nei servizi di cloud computing alla luce del nuovo Reg. 2016/679 UE* cit., pp. 381-382.

dall'art. 5, par. 2 del Regolamento, che richiede al titolare del trattamento di rispettare e dimostrare i principi applicabili al trattamento dei dati personali, nonostante la possibilità di ricorrere a certificazioni[183].

Se un sistema basato su richieste specifiche di autorizzazione sembra impercorribile, è altrettanto difficile per il *CSP* notificare ad ogni *data controller*/*client cloud* le variazioni nei *subproviders*/*subprocessors*, soprattutto in un ambiente *cloud* con molti utenti dove tali cambiamenti avvengono rapidamente. Per garantire che il *subcontracting* sia conforme al GDPR e che sia anche pratico, sono necessarie altre soluzioni. Il *CSP* potrebbe mantenere una lista permanente dei *subprocessors* a cui sono o potrebbero essere affidati i dati sulla nuvola, fornendo informazioni come estremi identificativi, breve descrizione del servizio subappaltato, localizzazione geografica dei *server* e informazioni sulle certificazioni adottate. Inoltre, dovrebbe avvisare automaticamente i *data controller* di eventuali cambiamenti in questa lista non appena accedono ai servizi *cloud*. Poiché è difficile per il *CSP* operante in un ambito pubblico selezionare i *subprocessors* in base alle diverse necessità di sicurezza dei vari clienti, sarebbe auspicabile garantire al cliente il diritto di recedere dal contratto nel caso in cui uno dei *subprocessors* non fornisca le garanzie di sicurezza e affidabilità ritenute indispensabili, oltre alla portabilità dei dati[184].

Il *processor* deve garantire che il *subprocessor* lo informi della sua intenzione di coinvolgere un *sub subprocessor*, in modo da poter comunicare al *data controller* l'inserimento del nuovo soggetto nella catena di trattamento dei dati. Sarebbe consigliabile che le modalità tecniche per adempiere a questo obbligo fossero dichiarate nel contratto tra le parti, possibilmente simili a quelle consigliate in precedenza. Il *processor* dovrebbe includere nel contratto con i *subprocessors* un diritto di veto o, in alternativa, un diritto di recedere dal rapporto nel caso in cui il *sub subprocessor* indicato non soddisfi i requisiti di sicurezza promessi agli utenti finali del servizio, così da evitare il rischio di responsabilità nei confronti di questi ultimi o il rischio di terminare il contratto. Anche se la normativa non affronta

[183] Cfr. Mantelero, *Il Cloud Computing* cit., pp. 524-525.
[184] Cfr. Valle, Russo, Bonzaghi, Locatello, *Struttura dei contratti e trattamento dei dati personali nei servizi di cloud computing alla luce del nuovo Reg. 2016/679 UE* cit., pp. 384-385.

esplicitamente l'ipotesi in cui il *subprocessor* intenda coinvolgere ulteriori *sub subprocessors*, è ragionevole ritenere che il *data processor*, responsabile delle violazioni degli obblighi di sicurezza dei dati, debba vigilare anche su questa scelta[185].

3.2 **Domotica: chi sono il titolare e il responsabile del trattamento?**

Le informazioni generate dagli *oggetti intelligenti* sono non solo quantitativamente, ma anche qualitativamente superiori a quelle che già condividiamo quotidianamente sul *Web*. Sistemi che un tempo erano separati possono ora essere facilmente collegati, creando ulteriori informazioni rispetto a quelle che l'utente intendeva effettivamente fornire. Questi meccanismi hanno due conseguenze opposte: da un lato, permettono una migliore *profilazione* dell'utente; dall'altro, portano spesso a giudizi errati e fuori contesto. Diventa quindi fondamentale considerare le circostanze in cui i dati personali sono raccolti. A questo proposito, l'articolo 22 assume particolare rilevanza, sancendo il diritto dell'interessato a non essere sottoposto a decisioni basate unicamente su trattamenti automatizzati, inclusa la *profilazione*, quando questi producano effetti giuridici o incidano significativamente sulla sua persona[186].

Al di là delle questioni terminologiche, risulta molto complesso applicare le definizioni di titolare e responsabile nel contesto dell'*Internet delle Cose* (*IoT*). Il sistema *IoT* coinvolge simultaneamente e in modo integrato numerosi attori: i produttori dei dispositivi, i gestori delle piattaforme, le applicazioni di terze parti, le aziende che offrono i dispositivi in affitto o *leasing*, e altri ancora. In questo contesto, risulta complicato distinguere tra *controller* e *processor*. Consideriamo, ad esempio, un produttore di un dispositivo intelligente che, anche dopo la commercializzazione e la vendita del dispositivo, continua a modificare gli scopi del trattamento dei dati o i destinatari della loro condivisione. In una situazione del genere, il produttore del

[185] Cfr. Valle, Russo, Bonzaghi, Locatello, *Struttura dei contratti e trattamento dei dati personali nei servizi di cloud computing alla luce del nuovo Reg. 2016/679 UE* cit., pp. 385-386.

[186] Cfr. F. Giovanella, *Le persone e le cose: la tutela dei dati personali nell'ambito dell'internet of things* in V. Cuffaro, R. Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, I ed., Torino, 2019, pp. 1217-1218.

dispositivo dovrebbe evidentemente essere considerato come *controller* (titolare del trattamento), secondo la definizione di titolare che indica "*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 dei dati personali*". Lo stesso ragionamento si può estendere anche ai gestori delle piattaforme, poiché questi soggetti sono in grado di decidere quali dati raccogliere, per quali scopi, come trattarli e così via[187].

L'argomento è estremamente complesso, soprattutto in relazione alla domotica, che è diventata un vero e proprio ecosistema in cui diverse componenti sono costantemente connesse e interagiscono tra loro, senza che l'utente abbia un reale controllo sull'intero processo di distribuzione dei dati. La procedura di raccolta e distribuzione dei dati per la successiva elaborazione è completamente fuori dal controllo dell'utente, che può quindi passare facilmente da utilizzatore consapevole a potenziale vittima di un sistema di cui è protagonista, ma anche soggetto di studio e monitoraggio. Inoltre, c'è il rischio di attacchi informatici mirati che possono sfruttare le vulnerabilità dei *server* di raccolta dati[188].

Il GDPR, basato su un approccio centrato sul rischio, richiede al titolare del trattamento di valutare i rischi associati alle proprie attività di trattamento dei dati. Tuttavia, nei contesti tipici dell'*Internet of Things* (*IoT*), emerge la compresenza di diversi soggetti che possono essere identificati come titolari del trattamento e che possono potenzialmente danneggiare l'interessato. L'opacità che caratterizza questi ambienti presenta due principali problematiche: la perdita di controllo sui dati da parte dell'interessato e la difficoltà per il titolare del trattamento di conformarsi al Regolamento.

In primo luogo, è importante analizzare la difficoltà di identificare correttamente il titolare e il responsabile del trattamento. Questa questione è stata affrontata in passato dal Gruppo di lavoro nell'*Opinion* 2/2013 sulle applicazioni per dispositivi intelligenti (WP 202) e nell'*Opinion* 8/2014 sui recenti sviluppi nell'*Internet degli*

[187] Cfr. Giovanella, *Le persone e le cose: la tutela dei dati personali nell'ambito dell'internet of things* cit., pp. 1234-1235.

[188] Cfr. M. Stochino, *Domotica smart, quello che i consumatori non sanno: così ci giochiamo privacy e sicurezza*, in Agenda digitale, pubblicato 1.07.2021, consultato il 28.05.2024.

oggetti del 16 settembre 2014 (WP 223). Nell'*Opinion* 2/2013, si spiegava come questi trattamenti coinvolgano una varietà di *stakeholder*, tra cui i produttori dei dispositivi, i fornitori di servizi di *hosting* come i *social network*, gli sviluppatori e altri soggetti terzi con interessi aggiuntivi.

In particolare, gli attori coinvolti sono molto diversificati: il produttore del dispositivo (*device manufacturer*) che lo crea; il fornitore del dispositivo (*device provider*) che lo vende; il fornitore di rete (*network provider*) che fornisce le risorse di rete necessarie; il fornitore della piattaforma (*platform provider*) che offre capacità di *storage*, elaborazione e gestione; e il fornitore dell'applicazione (*application provider*), che sviluppa e distribuisce le *app* agli utenti finali, utilizzando le risorse fornite dal *network provider*, dal *platform provider* e dal *device provider*. A questi si aggiungono altri soggetti terzi con ulteriori interessi. Distinguere correttamente chi tra questi sia il titolare del trattamento non è semplice, ma è cruciale poiché determina la suddivisione delle responsabilità[189].

Se consideriamo i dispositivi dell'*Internet of Things* (*IoT*), che sono connessi in rete e includono processi di archiviazione e gestione dati basati su un'architettura *cloud* (come gli assistenti vocali nel contesto domestico), l'applicazione delle regole del GDPR risulta piuttosto complessa. Secondo il già citato parere del Gruppo di lavoro art. 29 del 16 settembre 2014, n. 8 (precedente all'entrata in vigore del GDPR e focalizzato sui recenti sviluppi nel campo dell'*IoT*), gli utilizzatori di questi dispositivi sono considerati responsabili del trattamento dei dati. D'altro canto, i produttori e i fornitori dei *software* installati, e in determinate circostanze, le terze parti che interagiscono con il dispositivo (come una piattaforma di *e-commerce* che si interfaccia con un elettrodomestico *smart* per svolgere determinate funzioni) sono considerati titolari del trattamento dei dati[190].

Questa qualificazione, tuttavia, è in contrasto con il già citato parere del Gruppo di lavoro Art. 29 in relazione al *cloud computing*, dove si considera che il cliente del servizio *cloud* sia il titolare del trattamento: poiché i servizi *IoT* generalmente si

[189] Cfr. A. Blatti, *Responsabilità e accountability in materia di protezione dei dati personali,* Trento Law and technology research group, student paer n. 87, 2023, pp. 243-244.

[190] Cfr. E. Tuccari, *I soggetti del trattamento* in G. Magri, S. Martinelli, S. Thobani, *Manuale di diritto privato delle nuove tecnologie,* I ed., Torino, 2022, p. 192.

basano su infrastrutture *cloud*, ne risulta una discrepanza tra le due qualificazioni adottate dal Gruppo di lavoro Art. 29 nei differenti pareri. Per cercare di risolvere questa incertezza, è necessario partire dal presupposto che la qualificazione di titolare o responsabile del trattamento dipende dalla relazione esistente tra il soggetto e i dati, nonché dal grado di autonomia decisionale riconosciuto a tale soggetto. In quest'ottica, è utile considerare la tipologia di dati trattati dai dispositivi *IoT* e, a tal fine, risulta utile la classificazione elaborata dal Gruppo di lavoro Art. 29 in merito alla portabilità dei dati[191], che distingue tra dati forniti direttamente dall'utente (ad esempio, parametri di età e sesso inseriti in un *fitness tracker* indossabile), dati di osservazione generati dall'uso del dispositivo (ad esempio, la geolocalizzazione dell'utente) e dati inferiti dal dispositivo stesso (ad esempio, il profilo atletico dell'utente elaborato tramite analisi di big data). Per quanto riguarda l'uso dei dispositivi *IoT*, adattando le considerazioni espresse dal Gruppo di lavoro Art. 29 riguardo al *cloud computing*[192], il titolare è colui che "determina la finalità ultima del trattamento e decide in merito all'esternalizzazione di tale trattamento e alla delega ad un'organizzazione esterna delle attività di trattamento, in tutto o in parte. I clienti di servizi potrebbero non avere margine di manovra nel negoziare i termini contrattuali dell'uso dei servizi. In ogni caso, alla fine è il cliente che decide in merito all'assegnazione di parte o della totalità del trattamento a servizi *cloud* per scopi specifici". Una situazione simile si verifica quando un soggetto decide di delegare al proprio termostato intelligente la gestione della temperatura ambientale in base alle proprie abitudini, determinando così gli scopi per cui i dati della casa e i comportamenti dell'utente saranno trattati. Per quanto riguarda i dati forniti dall'utente e quelli di osservazione, si dovrebbe dunque considerare titolare l'utente del dispositivo, mentre per le informazioni derivanti da ulteriori elaborazioni autonome da parte del fornitore del prodotto (che solitamente persegue anche un fine proprio e autonomo) si potrebbe configurare una contitolarità.

[191] Cfr. Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, adottate il 13 dicembre 2016 e aggiornate il 5 aprile 2017, Bruxelles, pp. 9 s.

[192] Cfr. Article 29 Data Protection Working Party, *Parere 5/2012 sul cloud computng,* adottato il 1 luglio 2012, Bruxelles, pp. 9 s.

Seguendo questa ricostruzione, i problemi di accesso ai dati e di portabilità dovrebbero ridursi sostanzialmente, poiché il titolare può disporre direttamente dei dati senza dover ricorrere all'esercizio di diritti specifici. Inoltre, verrebbero meno le criticità legate ai dati di terzi (si pensi al caso di uno *smart-toy* acquistato dal genitore e usato dal figlio) e alla loro qualificazione da parte del fornitore del servizio, dal momento che sarebbe l'utente a regolare direttamente il rapporto con tali soggetti.

Al contrario, se si considera che il servizio fornito tramite il dispositivo *IoT* offra all'utente competenze specializzate tali da qualificare il fornitore del servizio come un titolare autonomo, si seguirà l'impostazione più recente adottata dal Gruppo di lavoro Art. 29 per la protezione dei dati, nel Parere 8/2014. Secondo questa interpretazione, sarà necessario ottenere il consenso dell'interessato al trattamento, che dovrà essere libero ai sensi dell'articolo 7, paragrafo 4, del Regolamento. A questo proposito, il Gruppo di lavoro Art. 29 ha correttamente osservato che "i meccanismi classici usati per ottenere il consenso delle persone possono essere difficili da applicare all'*IoT*. Pertanto, si ottiene un consenso di *bassa qualità*, basato su una mancanza di informazione o sull'impossibilità di fatto di dare un consenso ben calibrato che tenga conto delle preferenze espresse dalle persone". Inoltre, sul fornitore del servizio/titolare graveranno specifici obblighi riguardo alla conservazione e cancellazione dei dati raccolti. A tal proposito, il Gruppo di lavoro Art. 29 suggerisce che, qualora l'utente non utilizzi il servizio per un periodo di tempo determinato, il relativo profilo diventerà inattivo e, dopo un ulteriore periodo di tempo, i dati dovranno essere cancellati previa informazione dell'utente circa tali misure[193].

In aggiunta a ciò, è di particolare rilievo esplicare la successiva interpretazione di Vizzoni, conseguente all'eventuale contitotlarità presente nel *cloud computing*, citata nel precedente paragrafo. In questo caso, l'utente di un dispositivo domotico che utilizza il *cloud* potrebbe subire un cambiamento radicale nel suo ruolo, perdendo la qualifica di interessato e la possibilità di esercitare i relativi diritti. Tuttavia,

[193] Cfr. A. Mantelero, G. Vaciago, *Internet of things (IOT)* in in R. Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato: commentario al regolamento UE n.2016/79 (GDPR) e al novellato D. Lgs n. 196/2003 (Codice Privacy): scritti in memoria di Stefano Rodotà*, I ed., Milano, 2019, pp. 566-567.

configurare l'utente come la persona fisica che effettivamente determina le finalità e i mezzi del trattamento dei dati personali, come previsto dall'art. 4 del GDPR, risulta forzato e non in linea con la *ratio* del GDPR, soprattutto perché l'utente spesso non è consapevole del funzionamento del dispositivo né dell'esistenza stessa del *cloud*. Anche se si accetta che il cliente possa determinare la finalità dei dati forniti al *cloud provider*, le modalità di determinazione e controllo del trattamento sono sostanzialmente delegate ad altri. La proposta di qualificare l'utente come (co)titolare del trattamento imporrebbe ulteriori obblighi legati a tale ruolo, rendendo la situazione ancora più complessa per l'utente stesso[194].

Risulta utile osservare come il concetto di contitolarità si sia ampliato mentre quello dell'esenzione domestica si sia ristretto, in quanto i due concetti sono stati interpretati dalla Corte di Giustizia dell'Unione Europea. Di conseguenza, i proprietari di case intelligenti che scelgono di adottare una tecnologia progettata per migliorare la sicurezza e la *privacy* delle loro abitazioni possono correre un alto rischio di essere classificati come contitolari senza la protezione garantita dall'esenzione domestica. Sebbene la contitolarità e l'esenzione domestica siano due questioni legali separate, sono strettamente collegate poiché la prima stabilisce la soglia in cui un gruppo di entità è considerato collettivamente responsabile del trattamento dei dati, mentre la seconda esenta gli individui dal ruolo di titolari del trattamento se le attività in questione sono puramente personali o domestiche. Il GDPR chiarisce ulteriormente che l'esenzione si applica solo alle persone fisiche e non alle entità che forniscono i mezzi per tali attività. Pertanto, riguardo al trattamento dei dati coinvolto nell'invio di messaggi privati sui *social media*, ad esempio, i mittenti e i destinatari possono essere esentati dall'applicazione del GDPR, ma il fornitore del servizio di *social media* no. In altre parole, l'esenzione domestica è specifica per i titolari e mira a sollevare i privati dagli oneri di conformità.

Il concetto di contitolarità e l'esenzione domestica sono essenzialmente un meccanismo tutto o niente, escludendo le responsabilità per alcuni gruppi di utenti di

[194] Cfr. L. Vizzoni, *Domotica e diritto. La smart hometra regole e resposabilità,* I ed., Milano, 2021, pp. 80 s.

dati e imponendole esclusivamente ad altri gruppi. Questi due concetti seguono la logica secondo cui, se una persona è un titolare del trattamento e non qualificata per l'esenzione domestica, sarà responsabile a pieno titolo (o come parte di un pacchetto completo di responsabilità); altrimenti, non avrà alcuna responsabilità. Le responsabilità di ciascun contitolare, come spiegato di seguito, possono non essere identiche, ma senza una guida chiara, la contitolarità può comportare un notevole carico di oneri non proporzionati al ruolo di ciascun titolare. Nella misura in cui la contitolarità e l'esenzione domestica determinano chi deve e chi non deve essere ritenuto responsabile per le attività di trattamento dei dati, esse fungono da meccanismo legale per assegnare responsabilità.

Il modo in cui la contitolarità e l'esenzione domestica sono delineate nel GDPR riflette alcune assunzioni che potrebbero essere valide per una casa tradizionale, ma probabilmente non più per una casa intelligente. In primo luogo, si assume che le attività personali o domestiche siano per lo più confinate entro i limiti fisicamente discernibili di uno spazio privato. Ad esempio, la gestione di una rubrica di indirizzi solitamente avviene esclusivamente all'interno della propria casa e ha quindi un impatto minimo, se non nullo, sui contatti elencati. In secondo luogo, le responsabilità possono essere chiaramente definite e assegnate o rimosse in modo semplice a un gruppo specifico di persone. Nel caso di una rubrica di indirizzi, ad esempio, i detentori del libro sarebbero le uniche parti responsabili dell'uso della rubrica, il che non comporta questioni di responsabilità condivisa. In queste due condizioni, i due concetti possono funzionare in modo semplice: all'interno della casa, nessuna responsabilità; fuori dalla casa, piena responsabilità. Tuttavia, come sarà mostrato nel resto di questa sezione, queste due assunzioni non funzionano più in un contesto IoT[195].

La situazione di incertezza riguardo ai soggetti che trattano i dati personali ha un impatto significativo sulla possibilità per l'interessato di esercitare i propri diritti. Questi diritti rischiano di essere notevolmente compromessi se non viene correttamente identificato il soggetto nei confronti del quale possono essere

[195] Cfr. J. Chen, L.Edwards, L. Urquart, D. McAuley, *Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption*, in International Data Privacy Law, vol. 10, no. 4, 2020.

esercitati. Inoltre, alcuni diritti dell'interessato sembrano poco applicabili in contesti come quello dell'*IoT*. Un diritto rilevante in questo ambito è quello alla cancellazione dei dati, considerata la capacità dei dispositivi *IoT* di raccogliere, memorizzare e trasmettere a terzi grandi quantità di informazioni. Questo diritto diventa problematico anche per quanto riguarda gli oggetti usati, come nel caso di una vendita *B2B* di uno *smart home speaker* usato, che potrebbe aver raccolto molti dati personali del venditore, inclusi dati sulle abitudini di vita e sulla composizione familiare.

Tuttavia, l'applicazione di questo diritto presenta difficoltà specifiche, specialmente in relazione al comma 2 dell'articolo 17 del GDPR, che obbliga il titolare del trattamento, se ha reso pubblici i dati, a cancellarli tenendo conto della tecnologia disponibile e dei costi di attuazione. Il titolare deve adottare misure ragionevoli, anche tecniche, per informare gli altri titolari del trattamento della richiesta dell'interessato di cancellare qualsiasi *link*, copia o riproduzione dei suoi dati personali. Questa disposizione rende la posizione del titolare del trattamento più gravosa, imponendogli un obbligo informativo complesso da attuare, soprattutto in un contesto caratterizzato dalla complessità dei trattamenti e dalla molteplicità dei soggetti coinvolti[196].

3.2.1 *È possibile fare un'analogia con le self-driving cars?*

Quando si parla di *smart cars*, si entra in un discorso ampio che copre sia un futuro ormai prossimo, rappresentato dai veicoli autonomi (o *self-driving cars*) sia una realtà già consolidata con i sistemi informatici presenti nei veicoli attuali. Non ci riferiamo solo ai sistemi di navigazione satellitare che gestiscono i navigatori, monitorano il traffico e le condizioni meteorologiche, ma anche a dispositivi che registrano vari dati del veicolo, come la velocità, lo stato dei freni, l'angolo di sterzata, la posizione della valvola a farfalla, lo stato delle cinture di sicurezza e degli airbag, l'usura dei pneumatici e lo stile di guida, per migliorare l'efficienza complessiva del veicolo.

[196] Cfr. Vizzoni, *Domotica e diritto. La smart home tra regole e responsabilità* cit., pp. 82-84.

Questi sistemi intelligenti delle automobili sono progettati per raccogliere dati operativi relativi all'uso del veicolo con l'obiettivo di ottimizzare le prestazioni. Inoltre, tali sistemi permettono l'erogazione di nuovi servizi attraverso la telematica di bordo: oltre a fornire assistenza in caso di incidente, le case automobilistiche possono offrire servizi di geolocalizzazione, come la ricerca del parcheggio più vicino, il controllo remoto dello stato del veicolo e la prevenzione dei guasti. Questi servizi sono già disponibili tramite le applicazioni per *smartphone*[197].

I risultati del progetto *My Car My Data* indicano che i dati derivanti dalla connessione dei veicoli possono provenire sia dall'utente (dati forniti dal cliente) sia dal veicolo autonomo (dati generati dal veicolo). Nel primo caso, i dati sono indubbiamente personali e appartengono al proprietario del veicolo, al conducente o ai passeggeri a bordo. Questi dati includono, ad esempio, la localizzazione del veicolo e dei suoi passeggeri, i tragitti percorsi e le informazioni derivanti dalla sincronizzazione del cellulare degli utenti con l'auto connessa. Nel secondo caso, i dati sono prodotti dal veicolo stesso e possono essere personali o semplicemente tecnici. Secondo l'orientamento prevalente, che è di carattere restrittivo, rientrano nella categoria dei dati tecnici solo quei dati che non possono in alcun modo essere collegati all'utente; altrimenti si tratta di dati personali o sensibili. Ad esempio, un dato tecnico come il livello dell'olio nel motore del veicolo diventa un dato personale se può essere collegato a un utente specifico, poiché permette di fare deduzioni sulla sua sfera personale[198].

Questi dati non sono condivisi solo con altre vetture della flotta, per esempio per evitare ingorghi, ma anche con gli operatori della flotta di veicoli autonomi anche detti ACV. Pertanto, i veicoli autonomi illustrano perfettamente il potenziale ambivalente di questo tipo di trattamento dei dati, con applicazioni che spaziano da programmi di sicurezza socialmente e individualmente benefici a contratti sfruttatori. Mentre il dibattito legale attuale sui veicoli autonomi tende a concentrarsi su questioni di regolamentazione della sicurezza stradale e responsabilità civile per

[197] Cfr. A. C. Nazzaro, *Privacy, smart cities e smart cars* in E. Tosi (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy,* I ed., Milano, 2019, pp. 329-330.

[198] Cfr. M. C. Gaeta, *La protezione dei dati personali nell'internet of things: l'esempio dei veicoli autonomi* in *Il diritto dell'informazione e dell'informatica*, anno XXXIV, n.1, 2018, p. 156.

incidenti, qui si vuole evidenziare che la contrattazione sfruttatrice basata sui dati rappresenta un problema trascurato nel contesto degli *ACV*, e più in generale nell'intersezione tra IA e *IoT*.

I dati personali raccolti nei veicoli autonomi non includono solo i dati di geolocalizzazione; tecniche avanzate di riconoscimento vocale e analisi del parlato basate sull'IA, applicate alle conversazioni o ai comandi del veicolo registrati dal sistema di guida vocale di un *ACV*, permettono la costruzione di profili completi della personalità del parlante. Le specifiche interazioni dei conducenti con la guida automatizzata, come i modelli di frenata, possono essere analizzate per categorizzare i guidatori. Inoltre, scansionando l'ambiente, gli *ACV* raccolgono inevitabilmente dati su altri partecipanti al traffico come pedoni, ciclisti o altri conducenti. Se l'esperienza passata può fornire una guida, questi dati saranno utilizzati al massimo delle possibilità tecnologiche e legali dalle aziende che sviluppano *ACV* (operatori di *ACV*). Questi includono non solo i produttori di automobili, ma anche aziende come *Google*, *Apple* o *Uber*, il cui appetito per la raccolta, acquisizione e analisi dei dati personali è ben documentato. Non sorprende quindi che il Rapporto del 2015 del Forum Internazionale dei Trasporti presso l'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) osservasse: "I produttori potrebbero anche perseguire nuovi flussi di entrate tramite servizi di abbonamento all'automazione, pubblicità rivolta ai consumatori o la commercializzazione dei dati degli utenti". E il *Chief Digital Officer* di *BMW* affermava che la personalizzazione sarà un fattore chiave di valore aggiunto in futuro, sia "nel veicolo, sul dispositivo mobile, o in qualsiasi altro punto di contatto". Ciò è confermato da un'indagine del settore che rileva che il 28% delle aziende intende utilizzare i dati raccolti dai dispositivi legati all'*IoT* per prodotti e servizi personalizzati. Come suggerisce questo articolo, tale personalizzazione è probabile che abbia un effetto ambivalente sugli utenti, danneggiandone alcuni e beneficiandone altri. L'aumento dell'uso dei veicoli autonomi può quindi essere utilizzato come caso di studio per dimostrare le tensioni intrinseche tra innovazione e sfruttamento derivanti dalla raccolta dei dati personali nell'*IoT*[199].

[199] Cfr. P. Hacker, *Personal data, exploitative contracts, and algorithmic fairness: autonomous vehicles meet the internet of things* in International Data Privacy Law, 2017, Vol. 7, No. 4, pubblicato il 1.09.2017, consultato il 3.06.2024, pp. 267-268.

Sulla base della Dichiarazione di Amsterdam sulla cooperazione nel settore della guida connessa e automatizzata del 14 aprile 2016, la Commissione Europea, nella sua comunicazione sulla strategia europea per i sistemi di trasporto intelligenti cooperativi, ha sottolineato che la protezione dei dati personali è cruciale per il successo della diffusione dei veicoli cooperativi, connessi e automatizzati. Gli utenti devono essere certi che i loro dati personali non saranno usati come merce di scambio e devono avere il controllo reale sulle modalità e finalità di utilizzo dei loro dati. Secondo la Commissione, i dati trasmessi dai veicoli saranno generalmente considerati dati personali, poiché si riferiscono a una persona fisica identificata o identificabile, e quindi soggetti alla normativa sulla protezione dei dati. Per questo motivo, la protezione dei dati fin dalla progettazione e per impostazione predefinita (*privacy by design e by default*) e il *Data Protection Impact Assessment* sono essenziali per la progettazione dei sistemi di guida autonoma, specialmente in relazione alla sicurezza della comunicazione.

Il primo impegno condiviso da Stati membri, Commissione e Parlamento europeo è di sviluppare un quadro comune europeo per condividere esperienze e progressi, sfruttando appieno il potenziale della guida connessa e automatizzata. Questo quadro consentirà di analizzare le questioni relative all'uso dei dati personali pubblici e privati, con particolare attenzione alla definizione delle responsabilità dei soggetti coinvolti[200].

Parlando in concreto di soggetti del trattamento si può dire che il trattamento dei dati personali può riguardare il proprietario del veicolo, il conducente o un passeggero. La questione della titolarità dei dati (intesa come *ownership*) è intuitiva quando si tratta di dati forniti dal cliente, che sono riconducibili ai soggetti appena menzionati e, essendo dati personali, rientrano nell'ambito di applicazione del GDPR. Al contrario, quando si tratta di dati generati dal veicolo, se i dati sono personali, è abbastanza facile collegarli al soggetto interessato dal trattamento e, in quanto tale, titolare dei dati, risultando applicabile il GDPR. Tuttavia, quando i dati generati dal veicolo non sono dati personali ma meri dati tecnici, risulta difficile individuare il titolare e la normativa applicabile. Secondo una dottrina autorevole,

[200] Cfr. Mantelero, Vaciago, *Internet of Things (IOT)* cit., pp. 572-573.

sarebbe opportuno individuare il titolare dei dati in colui che ha un maggiore interesse negli stessi[201]. Per quanto riguarda la normativa applicabile, trattandosi di dati che esulano dall'applicazione del GDPR (in quanto non sono dati personali), si potrebbe ipotizzare l'introduzione di una normativa *ad hoc* per i dati generati dall'*IoT*, caratterizzati dalla loro novità. In questa categoria rientrerebbero i dati generati dalla connessione dei veicoli autonomi. Tuttavia, non è semplice introdurre una normativa così specifica a causa delle molteplici incognite relative alla materia da disciplinare e alla titolarità di tali dati.

Per quanto riguarda il titolare del trattamento, sembra preferibile la tesi secondo cui i titolari del trattamento possano essere il produttore del veicolo, il produttore di una componente elettronica del veicolo (compresa la scatola nera o il servizio *eCall*) o soggetti terzi, come ad esempio fornitori di servizi. Questi soggetti raccolgono dati non solo sulla *performance* dei propri prodotti o sull'andamento del mercato, ma anche dati personali degli utenti, che spesso ne sono inconsapevoli[202].

«Le automobili, ad esempio, stanno diventando una sorta di smartspeaker con le ruote. Anche in quel caso gli assistenti vocali dovranno essere progettati in modo corretto»[203]. Questa citazione di Stochino risulta utile per esprimere il fatto che la situazione delle *self-driving cars* sia analoga a quella della domotica sopra descritta, con tutte le implicazioni relative anche al contesto del *cloud.*

3.3 **Verso il futuro: i robot come soggetti del trattamento?**

Come già esplicato nel primo capitolo, articolo 26 introduce la figura dei contitolari nel sistema regolatorio, permettendo che uno stesso trattamento possa essere gestito da due o più soggetti che ne determinano congiuntamente finalità, modalità e mezzi. La norma, interpretata letteralmente, sembra riferirsi solo

[201] Cfr. T.J. Farkas, *Data created by the Internet of Things: the new gold without ownership*, in Rev. Prop. Inmaterial, vol. 23, 2017, pp. 7-8.

[202] Cfr. M. C. Gaeta, *La protezione dei dati personali nell'internet of things: l'esempio dei veicoli autonomi* in *Il diritto dell'informazione e dell'informatica* cit., pp, 156-157.

[203] V. M. Stochino, *Domotica smart, quello che i consumatori non sanno: così ci giochiamo privacy e sicurezza* in Agenda digitale, pubblicato il 1.07.2021, consultato il 10.06.2024.

all'ipotesi in cui ci sia un unico trattamento con più titolari, escludendo la possibilità che ci siano trattamenti distinti tra loro ma collegati da finalità comuni, gestibili da tutti o solo da alcuni dei contitolari.

Se la norma fosse intesa in questo senso stretto, risulterebbe inadatta a gestire la complessità dell'intelligenza artificiale, che spesso comporta una pluralità di trattamenti collegati tra loro e finalizzati a raggiungere obiettivi comuni. Tuttavia, è possibile interpretare la disposizione in modo più ampio, vedendo il "trattamento unico" come un insieme di trattamenti interconnessi, ciascuno con la propria finalità, ma tutti orientati verso uno scopo finale comune. In questo caso, i contitolari non sarebbero legati a trattamenti unitari per modalità e finalità specifiche, ma parteciperebbero a una catena di trattamenti uniti dallo scopo finale, rimanendo ciascuno responsabile per i trattamenti specifici di cui sono titolari. Attualmente, l'articolo 26 prevede che i contitolari siano legati da un accordo che definisca i loro ruoli e i rapporti con gli interessati, accordo che deve essere reso disponibile agli interessati almeno nei suoi aspetti essenziali. Inoltre, indipendentemente dall'accordo, l'interessato può esercitare i suoi diritti nei confronti di ciascun titolare del trattamento. La previsione di contitolari legati da un accordo appare adatta anche a gestire trattamenti frammentati ma coordinati, caratteristici di molte tecnologie legate all'intelligenza artificiale e alla robotica, aprendo scenari interessanti per la futura tutela dei dati personali. Non è improbabile pensare che, se mai dovesse emergere l'idea di un *robot* responsabile dei propri comportamenti e dotato di una propria "personalità elettronica", questo *robot* potrebbe essere considerato contitolare dei trattamenti che realizza, responsabile insieme agli altri contitolari, umani inclusi, per eventuali violazioni al GDPR. Questi scenari futuristici richiedono di pensare in grande e con lungimiranza, data la rapidità dell'evoluzione tecnologica.

È chiaro che ci troviamo di fronte a un Regolamento che privilegia la sostanza sulla forma, come dimostra l'importanza attribuita al titolare e alla sua responsabilità. Un'interpretazione troppo formale delle norme potrebbe essere in contrasto con gli obiettivi della nuova regolazione[204].

[204] Cfr. F. Pizzetti, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in F. Pizzetti, *Intelligenza artificiale, protezione dei dati personali e regolazione,* Torino, I ed., 2022, pp. 76-77.

Il tema dei registri dei trattamenti nelle tecnologie IA è complesso a causa delle loro numerose applicazioni. È probabile che si svilupperà una catena di responsabili dei trattamenti complessi, ciascuno responsabile di un segmento specifico. Alla fine della catena, ci saranno i responsabili finali, specialmente nell'IA applicata a *robot* e *IoT*, che determineranno gli effetti concreti sugli utenti e le persone coinvolte incidentalmente.

L'art. 30 del GDPR dovrà essere applicato da ogni responsabile della catena, ognuno con il proprio registro. È incerto se debbano registrare anche i collegamenti con altri trattamenti. L'aspetto più delicato riguarda le catene di trattamenti finalizzati a una fase operata da macchine "intelligenti" e robotiche connesse ai sistemi *IoT*. In questi casi, si pone il problema di chi debba tenere i registri dei trattamenti effettuati dalle macchine, specialmente quando utilizzano informazioni, personali o meno, raccolte nell'ambiente in cui operano autonomamente. Una possibile risposta è che le macchine debbano tenere una registrazione automatica dei trattamenti sulla base della loro capacità di analisi e delle decisioni prese. In questo quadro, il produttore o il fornitore della macchina potrebbero essere considerati responsabili della tenuta dei registri nei confronti dell'Autorità, il che implicherebbe che questi soggetti possano accedere in ogni momento, anche da remoto, alle registrazioni. Questo scenario comporta una possibilità costante di controllo remoto sull'attività delle macchine, che si traduce anche nella possibilità di controllo sui dati degli utenti e delle persone eventualmente coinvolte, i cui dati personali sono stati analizzati.

Non è pratico immaginare che l'utilizzatore della macchina, anche se spesso il proprietario, sia responsabile dei registri, a meno che l'EDPB non emetta Linee guida specifiche. Solo se l'utilizzatore può dare istruzioni specifiche alla macchina, l'obbligo di tenere i registri potrebbe ricadere su di lui. La difficoltà nel determinare chi debba tenere i registri nei sistemi IA e *IoT* mette in tensione il rapporto tra GDPR e tecnologia[205].

Nella risoluzione del Parlamento europeo del 16 febbraio 2017 si auspica l'istituzione di uno *status* giuridico specifico per i *robot* nel lungo termine, affinché almeno i robot autonomi più sofisticati possano essere considerati come "persone

[205] Cfr. Pizzetti, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale* cit., pp. 88-89.

elettroniche" responsabili di risarcire qualsiasi danno da loro causato. Si prevede, inoltre, il riconoscimento della personalità elettronica dei *robot* che prendono decisioni autonome o che interagiscono in modo indipendente con terzi. Su questo punto è necessario muovere una critica, sia dal punto di vista tecnico-scientifico, per quanto evidenziato in precedenza, sia dal punto di vista della tecnica legislativa. Tale scelta potrebbe infatti incentivare una totale deresponsabilizzazione del produttore e dell'ideatore, creando un pericoloso *laissez-faire*. Considerato che i produttori e gli ideatori operano su un mercato globale, con regole non uniformi e complicati incastri di "scatole cinesi" a livello mondiale, questa situazione potrebbe compromettere, in ultima analisi, il concreto risarcimento, per problemi legati all'effettiva solvibilità del debitore. Analogamente ad altre entità riconosciute nell'ordinamento giuridico, come enti o associazioni, i "*robot* autonomi più sofisticati" con status di "persone elettroniche" avrebbero capacità giuridica e di agire, nonché un'autonomia personale e patrimoniale, che permetterebbe loro di adempiere alle obbligazioni assunte e quindi di risarcire i danni. All'autonomia decisionale e di interazione con l'ambiente esterno corrisponderebbe un'autonomia patrimoniale.

La tesi della "personalità elettronica" risulterebbe molto più efficiente rispetto al tentativo di adattare schemi di responsabilità *standard* previsti nella prima proposta. Inoltre, potrebbe configurare un sistema funzionante qualora la capacità cognitiva e decisionale dei robot fosse assimilata a quella dei soggetti che, per età o per indebolimento psico-fisico, non sono chiamati a rispondere in prima persona dei danni provocati, ma sono sostituiti nella funzione risarcitoria da coloro che se ne prendono cura. Tutte le criticità evidenziate nella parte occidentale del mondo circa la creazione di una "personalità elettronica" non trovano riscontro, ad esempio, in Oriente[206].

Si è già ipotizzato che un *robot* con personalità elettronica possa essere responsabile dei trattamenti dei dati che effettua, ma la sua responsabilità ultima resta da definire. In tal caso, i *robot*, dotati di personalità elettronica, potrebbero tenere i registri dei trattamenti di dati in conformità all'art. 30 del GDPR e cooperare con le

[206] Cfr. R. Trezza, *Diritto e intelligenza artificiale: etica, privacy, responsabilità, decisione*, I ed., Pisa, 2020, pp. 56-57.

Autorità di controllo ai sensi dell'art. 31. Anche se questa prospettiva può sembrare distopica, potrebbe essere realizzabile e vantaggiosa per l'attuazione dell'art. 30 GDPR. L'art. 30, paragrafo 3, che permette la tenuta elettronica dei registri, si rivela lungimirante. La registrazione elettronica sarà utile quando le macchine robotiche e i dispositivi *IoT* dovranno tenere registri dei dati trattati durante le loro attività.

Questa impostazione solleva nuovi problemi. Se i *robot* o i dispositivi *IoT* sono responsabili del trattamento dei dati, ci saranno conseguenze oltre l'obbligo di tenuta dei registri. Ad esempio, dovranno fornire trasparenza e informativa agli interessati e permettere l'esercizio dei loro diritti, come l'opposizione e la limitazione del trattamento. La questione della responsabilità (*accountability*) dei *robot* o dei dispositivi *IoT* coinvolge l'etica delle macchine e le sanzioni. Le sanzioni non dovranno essere solo pecuniarie, ma potrebbero includere la disattivazione del *robot* o la modifica del suo algoritmo. La disattivazione temporanea o permanente potrebbe essere necessaria se un *robot* viola il GDPR o causa danni. Queste misure potrebbero comportare una sorta di "selezione darwiniana" delle macchine. È chiaro che tali scenari richiedono un ruolo crescente delle Autorità di controllo, che dovranno operare in stretta collaborazione.

In questo contesto, la tenuta dei registri dei trattamenti anche per le macchine robotiche o *IoT* non è solo un'ipotesi teorica, ma diventa essenziale per verificare le cause di eventuali violazioni[207].

Per quanto riguarda la protezione dei dati personali, è essenziale considerare il ruolo delle macchine robotiche, programmate con algoritmi che le abilitano ad apprendere e prendere decisioni basate su dati, molti dei quali personali, raccolti e trattati in funzione delle condizioni ambientali e delle persone con cui interagiscono. Nel contesto del Regolamento generale sulla protezione dei dati (GDPR), questa questione si concentra principalmente sulle responsabilità dei titolari del trattamento in merito ai danni potenziali che potrebbero causare. Tuttavia, il problema è analogo a quello della responsabilità civile legata alle azioni eseguite dalle macchine.

Questi due aspetti condividono punti in comune e differenze. Il punto in comune riguarda se e come si possa attribuire una forma di responsabilità a una macchina, il

[207] Cfr. Pizzetti, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale* cit., pp. 90-91.

che implica riconoscerle una sorta di personalità giuridica. La differenza risiede nel fatto che la nozione di titolare nel GDPR non è necessariamente legata a una persona fisica o giuridica, potendo essere un'autorità pubblica, un servizio o genericamente un organismo. Ciò che è cruciale per definire il concetto di titolare è che il soggetto in questione abbia il potere di determinare le finalità e i mezzi del trattamento dei dati personali (art. 4, paragrafo 1, numero 7). Pertanto, il punto centrale per stabilire se una macchina robotica possa essere considerata titolare del trattamento dei dati personali che influenzano le sue decisioni è determinare se essa abbia la capacità di decidere modalità e finalità del trattamento. Qualora si riconoscesse un ampio potere decisionale alle macchine, almeno per quanto riguarda i trattamenti che caratterizzano la fase finale della loro azione, non vi sarebbero ragioni per non considerare la macchina come titolare di fatto del trattamento ai sensi del GDPR, sebbene resti aperta la questione della sua responsabilità giuridica.

Nel caso in cui si stabilisse che la macchina è, in tutto o in parte, titolare dei trattamenti che esegue almeno nella fase finale delle decisioni relative alle modalità della sua azione, sorgerebbe il problema di come e in che misura essa possa adempiere ai doveri del titolare, primo fra tutti quello di trasparenza[208].

L'imprevedibilità e l'inevitabilità delle azioni compiute da dispositivi dotati di intelligenza artificiale super evolutiva interromperebbero il nesso di causalità tipico della responsabilità oggettiva per prodotti difettosi. Pertanto, oltre alle problematiche relative alla definizione di prodotto e alla sua tangibilità per l'applicazione della direttiva 85/374/CEE, emerge un'ulteriore questione di incompatibilità e responsabilità. Le disposizioni di questa direttiva porterebbero a considerare le "macchine" come "meri strumenti nelle mani di altri attori" (il fabbricante, l'operatore, il proprietario, l'utilizzatore), senza tenere conto dell'autonomia di cui sono dotate. Il primo modello definito nella risoluzione del febbraio 2017 si basa sul riconoscimento di una responsabilità oggettiva, richiedendo una "semplice prova del danno avvenuto e l'individuazione di un nesso di causalità tra il funzionamento lesivo del robot e il danno subito dalla parte lesa". Il secondo modello, invece, prevede una "gestione dei rischi", in modo da individuare il responsabile in colui che, tra i

[208] Cfr. Pizzetti, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale* cit., p. 172.

potenzialmente coinvolti, è in grado di minimizzare i rischi e ridurre l'impatto negativo. Quest'ultimo modello considera responsabile il soggetto che nella catena di produzione ha agito in ultima istanza, la cui responsabilità dovrebbe essere proporzionale al "livello effettivo di istruzioni impartite ai *robot*".

Non sembra dunque compatibile con gli attuali istituti giuridici una "responsabilità del *robot*" basata sulla personalità elettronica. Tuttavia, si potrebbe ipotizzare una scissione della responsabilità, ponendo da un lato la responsabilità del produttore o del formatore per l'errore o il malfunzionamento dell'algoritmo che ha causato il danno, e dall'altro una "responsabilità del *robot*" per il risarcimento di qualsiasi danno causato dalla propria autonomia. A sostegno di questa ipotesi di responsabilità oggettiva, il Parlamento europeo ha invitato la Commissione a nominare una squadra *ad hoc* per esaminare dettagliatamente la disciplina del risarcimento del danno, prevedendo due strumenti utilizzabili contemporaneamente o in maniera alternativa[209].

Un'altra ipotesi da considerare è quella di attribuire la qualifica di titolare del trattamento al produttore della macchina robotica. In questo scenario, il produttore, attraverso i programmatori che operano sotto la sua direzione, definisce gli algoritmi di funzionamento del dispositivo e stabilisce i limiti dei dati che la macchina può prendere in considerazione e delle decisioni che può assumere. Pertanto, sarebbe il produttore a dover essere considerato responsabile dei trattamenti effettuati dalle macchine da lui costruite e ad adempiere a tutti i doveri previsti dal GDPR nei confronti degli interessati. Adottando questa prospettiva, e tenendo conto che il *robot* possiede una capacità autonoma di prendere decisioni, almeno parzialmente, riguardo al raggiungimento delle finalità connesse ai trattamenti, si potrebbe ipotizzare di nominarlo come responsabile del trattamento ai sensi dell'art. 28 del GDPR. Va ricordato che il responsabile del trattamento tratta i dati per conto del titolare (art. 4, paragrafo 1, numero 8) e deve offrire garanzie sufficienti per implementare misure tecniche e organizzative adeguate per garantire che il trattamento soddisfi i requisiti del Regolamento e assicuri la tutela dei dati (art. 28, paragrafo 1). Questa ipotesi, a

[209] Cfr. Trezza, *Diritto e intelligenza artificiale: etica, privacy, responsabilità, decisione* cit., pp. 57-58.

prima vista, può sembrare una forzatura, ma, analizzandola più a fondo, risulta più sostenibile rispetto a quella che vede il *robot* come titolare, almeno di fatto, dei trattamenti. Tuttavia, un punto che potrebbe sollevare dubbi, oltre alla questione della personalità giuridica, è che la nomina del *robot* come responsabile implica che il titolare rimanga responsabile delle istruzioni impartite al responsabile, in questo caso il *robot*. Questo presuppone un legame costante e permanente tra il produttore, configurato come titolare, e il *robot*, nella sua qualità di responsabile.

Sarebbe curioso immaginare che un *robot* possa agire senza che chi lo ha prodotto mantenga la responsabilità per le attività da esso svolte, almeno per quanto riguarda le violazioni e i danni eventualmente provocati. La difficoltà di accettare l'ipotesi della macchina come responsabile del trattamento dei dati risiede nel grado di indipendenza che essa ha rispetto ai programmi che ne definiscono le modalità di funzionamento. È certamente più plausibile la nomina della macchina quale responsabile in sistemi in cui i programmatori mantengono una forma di vigilanza sui trattamenti dati eseguiti dalle macchine. È invece più complesso nei casi in cui la capacità delle macchine di apprendere e decidere sfugge, in tutto o in parte, anche al controllo dei programmatori[210].

3.4 **Profili critici delle IA generative**

Il 30 marzo 2023, il Presidente dell'Autorità italiana Garante per i dati personali ha preso una decisione d'urgenza nei confronti di *OpenAI*, la società dietro *ChatGPT*. Questa azione ha imposto la limitazione provvisoria del trattamento dei dati degli utenti italiani, mettendo in luce diverse problematiche legate alla protezione dei dati personali. La misura adottata dal Garante è stata motivata dalla scoperta di un *bug* in una libreria *open source* usata da *OpenAI*, che ha causato la pubblicazione non autorizzata di dati sensibili degli utenti. Questo incidente ha sollevato gravi preoccupazioni sulla sicurezza dei dati trattati da *ChatGPT*. Una delle

[210] Cfr. Pizzetti, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale* cit., pp. 173-174.

principali criticità rilevate è stata la mancanza di un'adeguata informativa agli utenti e a tutti gli interessati. *OpenAI* non ha fornito informazioni chiare su come i dati vengono raccolti e utilizzati. Questo ha impedito agli utenti di esercitare i propri diritti in materia di protezione dei dati. Due categorie principali di trattamenti sono state individuate: la raccolta e l'analisi dei dati necessari per la creazione del modello di linguaggio naturale, ossia i dati utilizzati per addestrare l'algoritmo di *ChatGPT*; l'elaborazione dei *prompt* degli utenti, cioè le interazioni con il *chatbot*.

Inoltre, il Garante ha contestato l'assenza di una base giuridica valida per la raccolta e la conservazione massiccia dei dati personali degli utenti. *OpenAI* non aveva giustificato adeguatamente queste operazioni, e il Garante ha chiesto di eliminare qualsiasi riferimento all'esecuzione di un contratto come base giuridica, suggerendo invece il consenso o il legittimo interesse, in linea con il principio di responsabilità previsto dal GDPR. Un altro punto critico riguardava la verifica dell'età. Il provvedimento ha richiesto a *OpenAI* di implementare meccanismi di verifica dell'età per proteggere i minori, con un piano di azione da attuare entro il 30 settembre 2023. Questo sistema doveva escludere l'accesso agli utenti sotto i tredici anni e ai minorenni senza il consenso dei genitori. Il Garante ha anche evidenziato problemi legati al principio di esattezza dei dati. *OpenAI* non permetteva agli utenti di esercitare i diritti di rettifica, cancellazione e opposizione. Questi diritti sono fondamentali per garantire che i dati personali utilizzati siano corretti e aggiornati.

In risposta alle misure imposte, *OpenAI* ha riaperto la piattaforma agli utenti italiani dopo aver implementato le richieste del Garante. Tra queste misure, c'era l'adozione di un'informativa trasparente sui trattamenti dei dati e sui diritti degli utenti. L'intera vicenda di *ChatGPT* evidenzia le sfide legate alla protezione dei dati personali nell'era dell'intelligenza artificiale. La mancanza di trasparenza, l'assenza di una base giuridica adeguata, la necessità di verificare l'età degli utenti e il rispetto del principio di esattezza dei dati sono problematiche centrali che devono essere affrontate. Questo caso sottolinea l'importanza di un quadro normativo chiaro ed efficace, capace di bilanciare l'innovazione tecnologica con la tutela dei diritti

fondamentali, con un ruolo attivo e coordinato delle autorità di controllo a livello nazionale ed europeo[211].

La regolamentazione dell'intelligenza artificiale presenta numerose sfide, soprattutto in termini di protezione dei dati personali. Un aspetto cruciale è rappresentato dai potenziali conflitti normativi: un sistema di IA può essere conforme alle regolamentazioni del GDPR, ma non alla nuova regolamentazione IA, causando possibili decisioni contrastanti tra le autorità competenti. Per risolvere tali conflitti, è stata proposta la creazione dell'Ufficio Europeo per l'Intelligenza Artificiale e l'introduzione di figure come il Coordinatore dell'Ufficio IA. Tuttavia, c'è preoccupazione riguardo alla sufficienza dei poteri di queste nuove autorità per gestire efficacemente tali conflitti.

La protezione dei dati personali è un tema centrale. La non conformità alle regolamentazioni sull'IA potrebbe abbassare gli standard di *privacy*, violando il diritto alla riservatezza. Questo è particolarmente problematico quando le violazioni dei dati sono *multi-offensive*, influenzando più ambiti regolatori e richiedendo competenze trasversali per essere affrontate adeguatamente. Per promuovere un'innovazione tecnologica rispettosa dei diritti umani, è necessaria una regolamentazione chiara e minima, orientata ai fatti tecnici e al principio di uguaglianza. È importante evitare che la paura legislativa ostacoli l'innovazione, favorendo invece una pazienza legislativa che bilanci adeguatamente innovazione e diritti fondamentali. Un'altra questione rilevante è la comunicazione efficace tra il nuovo Ufficio IA e le autorità nazionali regolatrici. Una migliore comunicazione è essenziale per garantire una regolamentazione coerente e trasparente. La regolamentazione dell'intelligenza artificiale è complessa e richiede cooperazione tra varie autorità regolatrici. Solo attraverso un approccio bilanciato e coordinato sarà possibile garantire che l'innovazione tecnologica avanzi in armonia con la protezione dei dati personali e altri diritti fondamentali[212].

---

[211] Cfr. L. Califano, *Chat gpt e Meta EDI: spunti problematici su profili regolatori e ruolo delle autorità di controllo di protezione dati* in Federalismi.it, pubblicato il 3.05.2023, consultato il 10.06.2024.

[212] Cfr. G. De Minico, *Too many rules or zero rules for Chat gpt?* In BioLaw journal-Rivista di Biodiritto, n. 2, 2023.

Nel contesto delle tecnologie basate sull'intelligenza artificiale (AI), come *ChatGPT*, sorge un dibattito cruciale riguardo alla protezione dei dati personali. Questi sistemi, inclusi gli *embeddings* utilizzati per comprendere e generare linguaggio naturale, dipendono dall'analisi di grandi quantità di dati per migliorare la loro capacità di interazione e risposta. Tuttavia, questo processo di apprendimento attraverso i dati solleva importanti preoccupazioni in termini di *privacy* e sicurezza. Gli *embeddings*, che rappresentano concetti e significati mediante vettori matematici, possono essere sensibili e rivelatori, specialmente quando applicati a dati personali. La raccolta, l'elaborazione e l'archiviazione di questi dati richiedono quindi un'adeguata protezione per evitare rischi di violazione della privacy e di uso improprio delle informazioni personali.

È essenziale che normative rigorose siano implementate per regolare l'uso e la gestione dei dati personali in ambienti IA. Queste normative dovrebbero non solo garantire la sicurezza dei dati durante il loro ciclo di vita, ma anche promuovere la trasparenza nell'uso degli *embeddings* e delle informazioni associate. Inoltre, l'adozione di pratiche di sicurezza e di gestione dei dati responsabili è fondamentale per costruire fiducia tra gli utenti e facilitare lo sviluppo etico e sostenibile delle tecnologie AI. In sintesi, mentre gli *embeddings* e le tecnologie IA come *ChatGPT* offrono opportunità significative per l'automazione e l'ottimizzazione dei servizi, è imperativo che vengano adottate misure robuste per proteggere la *privacy* e i diritti degli individui. Solo attraverso una regolamentazione efficace e un'impeccabile gestione dei dati, sarà possibile bilanciare l'innovazione tecnologica con la tutela dei diritti fondamentali nella società digitale contemporanea[213].

In conclusione, sembra logico pensare che il *chatbot* possa negli anni risultare anch'esso come soggetto del trattamento, o comunque rimane un entità che si frappone tra i soggetti, pur non prendendo decisioni, il suo comportamento potrebbe risultare influente ai fini del trattamento dei dati.

[213] Cfr, G. D'Acquisto, *Chatgpt e AI, regolamentare la responsabilità o l'efficienza è la prossima sfida* in Agenda Digitale, pubblicato il 18.04.2023, consultato il 10.06.2024.

Capitolo 4
CONCLUSIONI
IL FUTURO DEI SOGGETTI DEL TRATTAMENTO

4.1 **L'importanza della consulenza del Comitato europeo per la protezione dei dati personali (EDPB)**

L'apporto della consulenza dell'EDPB è facile da notare anche nei passaggi di questo elaborato. Precedentemente istituito come Working Party Article 29, appunto perché era introdotto dall'art. 29 della Direttiva 95/46, l'EPDB non si occupa solamente di pubblicare le linee guida atte a interpretare i profili più critici e paradigmatici del GDPR, ma anche delle controversie relative al trattamento transfrontaliero dei dati. Il lavoro del Comitato si traduce in pratica attraverso tre strumenti chiave: linee guida, raccomandazioni e prassi; pareri; decisioni vincolanti. Nell'esecuzione dei compiti e nell'esercizio dei poteri conferiti, il Comitato opera in modo autonomo e non richiede né accoglie istruzioni da terzi. Ogni questione che riguarda il GDPR può essere analizzata dall'EPDB su iniziativa volontaria oppure su richiesta di uno dei suoi membri o della Commissione Europea. Il Comitato europeo per la protezione dei dati deve consigliare la Commissione europea su qualsiasi argomento riguardante la protezione dei dati nell'UE, inclusa ogni proposta di modifica del GDPR e ogni proposta legislativa dell'UE. Deve anche consigliare la Commissione europea sul formato e le procedure per lo scambio di informazioni nel contesto delle norme vincolanti d'impresa.

Un altro compito importante del Comitato risiede nella valutazione del livello di sicurezza presente in un Paese terzo tramite pareri, per non dimenticare che si esprime anche su icone e certificazioni. Anche determinate decisioni dell'autorità di controllo sono soggette a questi pareri, per l'appunto fino a quel momento sono progetti di decisioni. Ulteriormente ci sono tre casi precisi in cui il Comitato deve prendere decisioni vincolanti: se un'autorità di controllo coinvolta ha sollevato un'obiezione a un progetto di decisione dell'autorità capofila o l'autorità capofila ha

rigettato tale obiezione (meccanismo di sportello unico); se ci sono opinioni divergenti su quale autorità di controllo sia l'autorità capofila; se un'autorità di controllo non richiede il parere del Comitato (parere necessario secondo il meccanismo di coerenza) o non si conforma al parere del Comitato[214].

L'apporto di queste misure è sempre molto importante, poiché permette al GDPR di non rimanere cristallizzato al passato, l'integrazione tra Regolamento, Comitato e Autorità di controllo comporta lo sviluppo di nuove linee interpretative. Anche se rimane vero che il Regolamento è quello e il mondo fuori è in continuo cambiamento. È fondamentale che ci sia continua collaborazione tra tutti questi attori e che ci sia un continuo aggiornamento su come funzionano gli ambiti tecnologici e soprattutto su come operano e come sono organizzate le aziende che ne governano le dinamiche. Visto che uno dei problemi principali è dato dal fatto che le aziende e i trattamenti di dati di conseguenza, sono organizzati in modi sempre più intricati e con un'organizzazione più di tipo reticolare piuttosto che verticistica.

4.2 **È necessario modificare il GDPR?**

In questo momento parrebbe avventato modificare il Regolamento, il fatto è che l'evoluzione in atto è in una fase ancora molto dinamica e si rischierebbe di arrivare a modificarlo nel momento in cui sarà già cambiato qualcos'altro. È pur vero che la struttura di tipo verticistico mal si adatta alle strutture dei soggetti attuali dei trattamenti. In un futuro prossimo bisogna pensare a come riformare la struttura del Regolamento in questo ambito, sicuramente è una sfida: uno spunto sarebbe quello di introdurre delle norme che regolino la situazione in cui l'interessato si trova nella posizione di titolare o responsabile del trattamento, improntandole in modo diverso a seconda che questo sia un'azienda con degli interessi in gioco o una persona fisica.

Sicuramente un punto di svolta potrà esserci se i *robot* saranno davvero messi in gioco come soggetti del trattamento, in quel caso potrebbe davvero non bastare l'assistenza del Comitato europeo per la protezione dei dati personali. Per il momento questa rimane sufficiente e fondamentale anche per dare una direzione al futuro del Regolamento: se quest'ultimo verrà mai modificato, tutta l'attività svolta

[214] Cfr. *Ruolo del Comitato europeo per la protezione dei dati* in epdb.europa.eu.

dal Comitato risulterà fondamentale. In tutto ciò questo Regolamento è in atto solo da sei anni, cambiarlo comporterebbe anche delle ricadute di tipo politico; risulta sicuramente più utile prevedere, come già succede, che anche i Codici di condotta e i Meccanismi di certificazione facciano la loro parte in questo processo. In aggiunta, l'Unione Europea ha legiferato su più fronti negli ultimi anni e l'interazione tra questi diversi regolamenti può creare sia soluzioni che altri casi paradigmatici.

4.3 **Il rapporto con il Regolamento e-privacy e Artificial Intelligence Act**

Risulta rilevante andare ad analizzare come coesistano i rapporti del GDPR con il futuro Regolamento e-privacy e con l'attuale Artificial Intelligence Act.

Tra il GDPR e il futuro Regolamento *e-Privacy* esiste una relazione in termini di *dipendenza*. Questa *dipendenza* implica che il GDPR svolga un ruolo centrale nella protezione dei dati personali, mentre la proposta *e-Privacy* supporta il GDPR specificamente nelle comunicazioni elettroniche. La direttiva 2002/58/CE segue la direttiva 95/46/CE, che regolava la protezione dei dati personali prima del GDPR. L'obiettivo del legislatore europeo con la proposta di regolamento *e-Privacy* è creare una normativa più adatta al contesto attuale e ai progressi tecnologici degli ultimi venti anni[215].

L'obiettivo principale dell'*Artificial Intelligence Act* è creare un ambiente sicuro che rispetti i diritti fondamentali nell'era dell'intelligenza artificiale. Si tratta di una missione ambiziosa volta a proteggere i pilastri della società europea, come i diritti umani, la democrazia, lo Stato di diritto e la sostenibilità ambientale. La nuova regolamentazione cerca di mitigare i rischi associati ai sistemi di IA con alto potenziale di impatto, stabilendo regole per l'immissione sul mercato e l'uso di tali sistemi, promuovendo al contempo l'innovazione e mantenendo l'Europa come punto di riferimento nel settore. Per assicurare che la definizione di intelligenza artificiale rimanga tecnologicamente neutrale e adattabile ai futuri progressi, la proposta di Regolamento include un elenco di tecniche e approcci per lo sviluppo dei sistemi IA,

[215] Cfr. N. Fabiano, *ePrivacy, il rapporto con la Direttiva 2002/58/CE e il GDPR* in Agenda Digitale, pubblicato il 1.03.2022, consultato il 10.06.2024.

aggiornato periodicamente dalla Commissione per tenere conto delle nuove tecnologie.

La normativa si applica a enti pubblici e privati, sia all'interno che all'esterno dell'UE, e riguarda tutti i fornitori e operatori che commercializzano o utilizzano sistemi di intelligenza artificiale nel territorio dell'Unione, inclusi quelli situati in Paesi terzi se il prodotto è utilizzato nell'Unione. Gli importatori devono garantire che i fornitori stranieri abbiano eseguito la procedura di valutazione di conformità, che il sistema abbia una marcatura di conformità europea e sia corredato dalla documentazione richiesta. L'*AI Act* non si applica ai sistemi di intelligenza artificiale utilizzati esclusivamente per scopi militari, di difesa o di sicurezza nazionale, né per attività di ricerca, sviluppo e prototipazione che precedono l'immissione sul mercato, né alle persone che usano l'IA per motivi non professionali[216].

In relazione al trattamento di dati personali, è interessante approfondire l'art. 5 dell'*AI Act*, che stabilisce i divieti per alcune pratiche legate all'uso dell'intelligenza artificiale. Sono proibite quattro principali pratiche. La prima riguarda l'immissione sul mercato, l'implementazione o l'uso di sistemi di IA che utilizzano tecniche subliminali per influenzare inconsciamente il comportamento delle persone, causando potenzialmente danni. La seconda concerne l'uso di sistemi di IA che sfruttano le vulnerabilità di gruppi specifici, come quelli con disabilità fisiche o mentali, per distorcere il loro comportamento, causando possibili danni fisici o psicologici. La terza pratica vieta l'uso di sistemi di IA da parte delle autorità pubbliche per valutare o classificare l'affidabilità delle persone nel tempo basandosi sul loro comportamento sociale o sulla personalità. Questo sistema di *social scoring* può portare a trattamenti ingiusti o sproporzionati, con l'obiettivo di prevenire discriminazioni ed esclusioni sociali. Infine, la quarta pratica proibisce l'uso di sistemi di identificazione biometrica remota e in tempo reale in spazi pubblici, eccetto nei casi di ricerca di vittime di reati, prevenzione di minacce imminenti o individuazione di sospetti di gravi reati punibili con almeno tre anni di carcere.

[216] Cfr. I. Carantani, *IA Act: l'Unione Europea approva la proposta di Regolamento sull'intelligenza artificiale* in Iusinitinere.it, pubblicato il 3.05.2024, consultato il 14.06.2024.

Gli orientamenti etici del Gruppo di esperti sottolineano i rischi del *social scoring*, indicando che le valutazioni dovrebbero essere giustificate e proporzionate, e suggeriscono che dovrebbero esistere modalità per dissociarsi da tali meccanismi senza pregiudizi. Gli Stati membri possono inoltre determinare specifici casi e situazioni in cui l'uso di questi sistemi è lecito[217].

L'interazione tra l'*AI Act* e il GDPR pone enfasi sulle valutazioni d'impatto necessarie per garantire la protezione dei dati personali e la sicurezza dei sistemi di intelligenza artificiale. Entrambi i regolamenti mirano a tutelare i diritti fondamentali delle persone, richiedendo specifiche misure di trasparenza e responsabilità per i titolari del trattamento dei dati. L'*AI Act* introduce la valutazione di impatto sui rischi (*FRIA*) per i sistemi di intelligenza artificiale ad alto rischio, simile alla *DPIA* (valutazione d'impatto sulla protezione dei dati) prevista dal GDPR. In alcuni casi, la *FRIA* può essere integrata con la *DPIA*, a condizione che siano rispettate le normative dell'articolo 29a dell'*AI Act*. Un punto cruciale riguarda la trasparenza e la base giuridica per la raccolta e il trattamento dei dati personali. Mentre il GDPR richiede una giustificazione chiara e trasparente per ogni trattamento di dati personali, l'*AI Act* vieta esplicitamente alcune pratiche, come l'uso di tecniche manipolatorie o la sorveglianza di massa, ma prevede eccezioni per motivi di sicurezza pubblica.

Entrambi i regolamenti puntano alla responsabilizzazione degli operatori. Il GDPR non elenca trattamenti vietati specifici ma si basa sulla responsabilità dei titolari del trattamento, mentre l'*AI Act* specifica chiaramente le tecniche e gli usi vietati per i sistemi di intelligenza artificiale. L'armonizzazione tra il GDPR e l'*AI Act* è essenziale per garantire la protezione dei dati personali e la sicurezza nell'uso dei sistemi di intelligenza artificiale, mantenendo un approccio centrato sull'individuo e sui suoi diritti fondamentali[218].

[217] Cfr. G. Proiettti, *Una normativa per l'intelligenza artificiale. La proposta di regolamento europeo* in Responsabilità d'impresa e antiriciclaggio, n.2, 2021, pp. 203-204.

[218] Cfr. D. Fulco, *AI Act e GDPR come si rapportano: "valutazione d'impatto" e DPIA* in Agenda Digitale, pubblicato il 25.03.2024, consultato il 10.06.2024.

4.4 **Codici di condotta e meccanismi di certificazione come possibile apporto a questi profili critici**

È già stato accennato come questi due elementi siano rilevanti per regolare diversi profili critici. Visto che è dalle stesse aziende che parte la modalità di organizzare i trattamenti e la distribuzione dei diversi attori, è importante che siano loro ad avviare la collaborazione per scrivere i codici di condotta. Questi sono strumenti molto importanti, perché, a differenza del Regolamento, si adattano alle specifiche dei settori di appartenenza e danno una guida per rispettarlo in modo preciso, sono anche utili per informare chi lavora nelle aziende. Collegandosi al discorso del paragrafo 3.3 si può ipotizzare che questi codici siano integrati nei *robot* e nei congegni dell'*IoT* tramite l'algoritmo con cui funzionano, cosi come per le IA generative.

Passando ai meccanismi di certificazione, il discorso è lievemente diverso. Una soluzione è rappresentata in parte dai meccanismi di certificazione introdotti con il *Cybersecurity Act.* Il primo programma adottato nell'ambito del quadro di certificazione del *Cybersecurity Act* si basa sul celebre *standard* internazionale *Common Criteria*, utilizzato per rilasciare certificati in Europa da quasi tre decenni. Lo schema sfrutta l'elevata reputazione dei fornitori e dei certificati europei usando la certificazione basata su *Common Criteria* in tutto il mondo.

Il sistema sarà applicato su base volontaria a livello dell'UE e si focalizzerà sulla certificazione della sicurezza informatica dei prodotti *TIC* nel loro ciclo di vita: sistemi biometrici, *firewall* (*hardware* e *software*), piattaforme di rilevamento e risposta, *router*, *switch*, *software* specializzati (come sistemi *SIEM* e *IDS/IDP*), diodi di dati, sistemi operativi (anche per dispositivi mobili), archivi crittografati, banche dati nonché *smart card* ed elementi di sicurezza inclusi in tutti i tipi di prodotti, come nei passaporti usati quotidianamente dai cittadini[219].

Questo regolamento assegnerà nuovi compiti e risorse all'agenzia europea per la sicurezza informatica, *Enisa*, e introdurrà una certificazione obbligatoria per i dispositivi connessi. L'obiettivo è stabilire standard di sicurezza per i dispositivi connessi, prevenendo attacchi informatici che possono sfruttare vulnerabilità come le *backdoor*. Uno studio ha rilevato che tra il 2013 e il 2017 gli attacchi *hacker* in

[219] Cfr. *Il quadro di certificazione della cibersicurezza dell'UE* in digital-strategy.ec.europa.eu.

Europa sono quintuplicati, colpendo non solo i computer ma anche dispositivi *smart* presenti nelle case. Il *Cybersecurity Act* darà all'*Enisa* più poteri e risorse per intervenire in caso di attacchi e definire le regole di certificazione[220].

In particolare, per i prodotti dell'*Internet of things* può rappresentare una buona soluzione per rassicurare sullo *storage* dei dati, e in questo caso sarebbe utile anche ad attuare la *privacy by design*. Anche da qui è rilevante capire come l'interazione tra *Cybersecurity Act* e GDPR crei delle possibili soluzioni.

4.5 **Una breve riflessione finale: la divulgazione di questa materia è fondamentale**

Infine, sembra doveroso dedicare una breve riflessione riguardo un aspetto importante: la divulgazione di questa materia. Secondo l'opinione dell'autore, la protezione dei dati personali è ancora un argomento che non desta troppa attenzione da parte degli interessati. Sarebbe importante che le persone sviluppassero una certa sensibilità verso la materia, in modo che siano i primi a pretendere il rispetto del GDPR e che i loro dati siano soggetti ad un'adeguata protezione.

Questo di tipo di informazione dovrebbe arrivare a più persone anche tramite una comunicazione, come delle campagne televisive, come già si fa per il consumo di alcool, per esempio; è vero che si tratta di due cose molto diverse, però il concetto di fare informazione per evitare comportamenti potenzialmente lesivi della persona è lo stesso. Contemporaneamente è vero che sul sito del Comitato europeo è possibile farsi una solida base di informazione, ma, parlando chiaramente, è difficile che il singolo di sua spontanea volontà si metta in moto per informarsi.

È fondamentale che questa materia diventi un elemento presente nella cultura generale delle persone, che non rimanga un *oggetto misterioso* paragonabile appunto all'informativa *privacy*, che rimane sempre poco letta e accettata in modo molto frettoloso. Non sarà mai possibile che tutti la leggeranno per intero e capendola, ma se almeno tutte le persone fossero in grado di comprendere quei passaggi

[220] Cfr. M. Longhin, *IoT, Smart devices e Smart houses: vantaggi, criticità e assenza normative*, in Iusinitinere.it, pubblicato il 19.02.2020, consultato il 25.06.2020.

fondamentali per valutarne la correttezza, sarebbe un bel passo in avanti. Citando poi i casi di cui si è parlato nel terzo capitolo, viene anche da chiedersi quando è presente davvero la consapevolezza negli interessati di essere alle volte considerati titolari o responsabili del trattamento, e ancor più rilevante quante persone sappiano davvero il significato di questi termini. In aggiunta, sarebbe ancora più importante e fondamentale trasmettere la consapevolezza di quando si ritrovano in mano dati sensibili, come può essere una banale foto imbarazzante mandata per scherzo su *whatsapp.*

In conclusione, questo aspetto potrà sembrare quello più trascurabile e meno pratico, ma in realtà è forse quello su cui più ci si debba impegnare, finché non sarà diffusa una consapevolezza generale, sarà difficile che i cittadini esigano il rispetto di questo Regolamento.

BIBLIOGRAFIA

1. **Fonti**

Amigoni Francesco, Schiaffonati Viola, Somalvico Marco, *Intelligenza artificiale* in Enciclopedia della scienza e della tecnica Treccani, 2008.

Artusio Claudio, Senor Monica A., The Law of Service Robots *Ricognizione dell'assetto normativo rilevante nell'ambito della robotica di servizio: stato dell'arte e prime raccomandazioni di policy in una prospettiva multidisciplinare,* Torino, Nexa Center for internet and society(PoliTO), 2015.

Balbi Giuliano (a cura di), *Diritto penale e intelligenza artificiale: nuovi scenari*, Torino, Giappichelli, 2022.

Barba Angelo, Pagliantini Stefano (a cura di), *Commentario del diritto civile, modulo delle persone*, volume II, Milano, Wolters Kluwer, 2019.

Blatti Andrea, *Responsabilità e accountability in materia di protezione dei dati personali,* Trento Law and technology research group, student paer n. 87, 2023.

Bolognini Luca, Pelino Enrico, Bistolfi Claudia, *Il regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali,* Milano, Giuffrè, 2016.

Buttarelli Giovanni, *A smart approach: counteract the bias in artificial intelligence*, in www.edps.europa.eu, pubblicato il 8.11.2016.

Cadoppi Alberto, Canestrari Stefano, Manna Adelmo, Papa Michele, *Cybercrime*, Milano, Wolters Kluwer, 2019.

Califano Licia, Colapietro Carlo, *Innovazione tecnologica e valore della persona: il diritto alla protezione dei dati personali nel Regolamento 2016/679*, Napoli, Editoriale Scientifica, 2017.

Cassano Giuseppe, Colarocco Vincenzo, Gallus Giovanni B., Micozzi Francesco, *Il processo di adeguamento al GDPR aggiornato al d.lgs 10 agosto 2018 n. 101,* Milano, Giuffrè Francis Lefebvre, 2018.

Cuffaro Vincenzo, Ricciuto Vincenzo, *La disciplina del trattamento dei dati personali*, Torino, Giappichelli, 1997.

Cuffaro Vincenzo, D'Orazio Roberto, Ricciuto Vincenzo, *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019.

D'Acquisto Giuseppe, Naldi Maurizio, *Big data e privacy by design: anonimizzazione, pseudonimizzazione, sicurezza*, Torino, Giappichelli, 2018.

D'Auria Massimo, *I problemi dell'informazione nel diritto civile, oggi*, Roma, Roma Tre-press, 2022.

Floridi Luciano, *La quarta rivoluzione: come l'infosfera sta trasformando il mondo*, Milano, Cortina, 2017.

Fumagalli Meraviglia Marinella (a cura di), *Diritto alla riservatezza e progresso tecnologico. Coesistenza pacifica e scontro di civiltà?*, Napoli, Editoriale Scientifica, 2015.

Magri Geo, Martinelli Silvia, Thobani Shaira (a cura di), *Manuale di diritto privato delle nuove tecnologie*, Torino, Giappichelli, 2022.

Il quadro di certificazione della cibersicurezza dell'UE in digital-strategy.ec.europa.eu.

Mantelero Alessandro, *Il costo della privacy tra valore della persona e ragione d'impresa*, Milano, Giuffrè, 2007.

McCorduck Pamela, *Storia dell'intelligenza artificiale: gli uomini, le idee, le prospettive*, I ed., Trento, Muzzio, 1987.

National Institute of Standards and Technology (NIST) *Definition of Cloud Computing, U.S. Department of Commerce*, Special Publication SP800-145, 2011.

Negri Carlo, *Come funziona l'AI generativa: significato e applicazioni* in Osservatori.net in collaborazione con Politecnico di Milano, ultimo aggiornamento 16.05.2024.

Panetta Rocco (a cura di), *Circolazione e protezione dei dati personali, tra libertà regole del mercato: commentario al regolamento UE n. 2016/679 e al novellato D.lgs. 196/2003, scritti in memoria di Stefano Rodotà,* Milano Giuffrè Francis Lefebvre, 2019.

Pizzetti Franco, *Privacy e diritto europeo: dalla Direttiva 95/46 al nuovo Regolamento Europeo*, Torino, Giappichelli, 2016.

Pizzetti Franco, *Intelligenza Artificiale, protezione dei dati personali e regolazione*, Torino, Giappichelli, 2018.
Rodotà Stefano, *Tecnologie e diritti*, Bologna, Il mulino, 1995.
Ruolo del Comitato europeo per la protezione dei dati in epdb.europa.eu.
Santosuosso Amedeo, *Intelligenza artificiale e diritto: perché le tecnologie di IA sono una grande opportunità per il diritto*, Firenze, Mondadori, 2020.
Sovalmico Marco, *Intelligenza artificiale* in *Progetto di Intelligenza artificiale e robotica,* Politecnico di Milano, 1987.
Tosi Emilio (a cura di), *Privacy digitale: riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffrè Francis Lefebvre, 2019.
Trezza Remo, *Diritto e intelligenza artificiale: etica, privacy, responsabiltà, decisione*, Pisa, Pacini Giuridica, 2020.
Vaswani Ashish, Shazeer Noam, Parmar Niki, Uszkoreit Jakob, Jones Llion, Gomez Aidan N., Kaiser Lukasz, Polosukhin Illia, *Attention is all you need* in *Advances in Neural Information Processing Systems*, Long Beach (California), 30esima ed., 2017, pp. 5998-6008.
Vizzoni Lavinia, *Domotica e diritto : la smart home tra regole e responsabilità*, Milano, Giuffrè Francis Lefebvre, 2021.

2. **Articoli di riviste giuridiche**

Brizzi Francesco, *Il GDPR in ambito giudiziario: fino a che punto può spingersi l'accountability* in Ius Penale GFL, 11.12.2018.
Bucci Francesca, *IoT e privacy:il problema della logica plug and play* in Iusinitinere.it, pubblicato il 7.04.2021.
Califano Licia, *Chat GPT e Meta EDI: spunti problematici su profili regolatori e ruolo delle autorità di controllo di protezione dati* in Federalismi.it, editoriale 3.05.2023.
Calzolaio Simone, *Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679* in Federalismi,it, edizione 20 dicembre 2017.
Capilli Giovanna, *Responsabilità e robot* in La nuova giurisprudenza civile commentata, anno XXXV, n. 3, 2019.

Carrozza Maria C., Oddo Calogero, Orvieto Simona, Di Minin Alberto, Montemagni Gherardo, *AI: profili tecnologici Automazione e Autonomia: dalla definizione alle possibili applicazioni dell'Intelligenza Artificiale* in BioLaw-Rivista di Biodiritto, n, 3/2019.

Cedrola Simone, *GDPR in the cloud: who is who?* in Iusinitinere.it, pubblicato il 3.11.2019.

Chen Jiahong, Edwards Lilian, Urquart Lachlan, McAuley Derek, *Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption*, in International Data Privacy Law, vol. 10, no. 4, 2020.

Carantani Isabella, *IA Act: l'Unione Europea approva la proposta di Regolamento sull'intelligenza artificiale* in Iusinitinere.it, pubblicato il 3.05.2024.

D'acquisto Giovanni, *Chatgpt e AI, regolamentare la responsabilità o l'efficienza è la prossima sfida* in Agendadigitale, pubblicato il 18.04.2023.

Di Viggiano Pasquale L., *Etica, robotica e lavoro: profili d'informatica giuridica* in Revista Opinião Jurídica (Fortaleza), n.22, 2016.

De Mari Casareto dal Verme Tommaso, *Rischio da circolazione stradale, R.C. auto e veicoli a guida autonoma* in BioLaw Journal-Rivista di Biodiritto, n.3/2023.

De Minico Giovanna, *Too many rules or zero rules for Chat gpt?* In BioLaw journal-Rivista di Biodiritto, n. 2, 2023.

Fabiano Nicola, *ePrivacy, il rapporto con la Direttiva 2002/58/CE e il GDPR* in Agenda Digitale, pubblicato il 1.03.2022.

Farkas Thomas J., *Data created by the Internet of Things: the new gold without ownership*, in Rev. Prop. Inmaterial, vol. 23, 2017.

Fulco Diego, *AI Act e GDPR come si rapportano: "valutazione d'impatto" e DPIA* in Agenda Digitale, pubblicato il 25.03.2024.

Gaeta Maria C., *La protezione dei dati personali nell'internet of things: l'esempio dei veicoli autonomi in Il diritto dell'informazione e dell'informatica*, anno XXXIV, n.1, 2018.

Hacker Philip, *Personal data, exploitative contracts, and algorithmic fairness: autonomous vehicles meet the internet of things* in International Data Privacy Law, 2017, Vol. 7, No. 4, pubblicato il 1.09.2017.

Limiti Chiara, *Intelligenza artificiale: implicazioni etiche in termini in materia di privacy e diritto penale* in Iusinitinere.it, 9.02.2021.

Longhin Michele, *IoT, Smart devices e Smart houses: vantaggi, criticità e assenza normative*, in Iusinitinere.it, pubblicato il 19.02.2020

Pizzetti Franco, *L'intelligenza artificiale che ci spia a casa: quali rischi e soluzioni per la privacy* in Agenda Dgitale, pubblicato il 4.07.2018.

Portinale Luigi, Intelligenza artificiale: storia, progressi e sviluppi tra speranze e timori in MediaLaws, 28.02.2022.

Proiettti Giuseppe, *Una normativa per l'intelligenza artificiale. La proposta di regolamento europeo* in Responsabilità d'impresa e antiriciclaggio, n.2, 2021.

Settimio Rosy, *Obblighi e responsabilità dei soggetti del trattamento: titolare e responsabile a confronto* in Giustiziacivile.com, 18.03.2022.

Spera Pierluigi, *Inadempimento del DPO* in Ius responsabilità civile Gfl, 18.10.2021.

Stochino Maurizio, *Domotica smart, quello che i consumatori non sanno: così ci giochiamo privacy e sicurezza*, in Agenda Digitale, pubblicato 1.07.2021.

Valle Laura, Russo Barbara, Bonzagni Guido, Locatello Davide M., *Struttura dei contratti e trattamento dei dati personali nei servizi di cloud computing alla luce del nuovo Reg. 2016/679 UE* in Contratto e Impresa/Europa, anno XXIII, pubblicazione annuale, 2018.

Vizzoni Lavinia, *Smart assistant e dati personali: quali rischi per gli utenti?* In Media Laws, n.2, 2020.

3. **Articoli di giornale online**

Di Tonto Giuseppe, *Intelligenza artificiale e nuovi diritti. Il caso chat gpt in Il bollettino di Clio*, n.19, 2023.

Casini Stefano, *Intelligenza artificiale, crescita record del mercato in Italia (+52%): in 10 anni sostituirà il lavoro di circa 3,8 milioni di persone* in Innovation Post, pubblicato il 1.02.2024.

Guidi Paola, *Risparmio ed efficienza: è la corsa della domotica* in Il Sole 24 Ore, Milano, pubblicato il 23.09.2023.

La Trofa Francesco, *Il business della robotica: prospettive e analisi di mercato* in Tech4future, pubblicato il 24-06.2022.

Mckinsey and Company, *Autonomous driving's future: convenient and connected*, pubblicato il 6.01.2023.
Synergy Research group , *Half-Yearly Review Shows $150 billion Spent on Cloud Services and Infrastructure*, , Reno, pubblicato il 19.09.2019,
Rusconi Gianni, *Quanto vale l'intelligenza artificiale generativa? Impatto potenziale da 4,4 migliaia di miliardi di dollari* in Il Sole 24 ore, pubblicato il 24.06.2023.