

Dipartimento  
di Giurisprudenza

Cattedra di Informatica Giuridica

IA e protezione dei dati personali  
Problemi giuridici sollevati dagli algoritmi di  
IA per il trattamento automatico dei dati

Prof. Stefano Russo

---

RELATORE

Prof. Ciacci Gianluigi

---

CORRELATORE

Marco Marozzo

---

CANDIDATO

Anno Accademico 2022/2023

*Alla mia famiglia,*

*in particolare ai miei genitori,  
ai miei nonni,  
a mia sorella Claudia,  
e a mio cugino Francesco,  
per avermi supportato ed incoraggiato  
per tutto il mio percorso accademico;*

*Ai miei cari amici e compagni di studi,  
per aver affrontato insieme questa esperienza di vita,  
superando ogni difficoltà e creando dei bellissimi ricordi.*

<b>Considerazioni introduttive</b> .....	
<b>1. Quadro generale dell'intelligenza artificiale</b> .....	
1.1. Nozione di intelligenza artificiale e machine learning .....	
1.2. Evoluzione dell'intelligenza artificiale .....	
1.3. I profili etici dell'intelligenza artificiale .....	
1.4. Rapporti fra il diritto e l'intelligenza artificiale .....	
<b>2. Quadro generale ed evoluzione della disciplina della privacy</b> .....	
2.1. Ricognizione della disciplina europea.....	
2.2. Disciplina nazionale .....	
2.3. Cenni introduttivi al GDPR.....	
<b>3. Intelligenza artificiale e trattamento automatizzato dei dati personali</b> .....	
3.1. Il Regolamento generale sulla protezione dei dati .....	
3.2. Il trattamento automatizzato.....	
3.3. Il consenso dell'interessato .....	
3.4. La profilazione e pseudonimizzazione.....	
3.5. Il titolare e il responsabile del trattamento .....	
3.6. Il processo decisionale automatizzato e l'intervento umano.....	
<b>4. Proposta di regolamento UE in materia di AI</b> .....	
4.1. Riflessioni sui 'Motivi e obiettivi della proposta' .....	
4.2. La struttura generale della 'proposta' .....	
4.3. Le metodologie di armonizzazione della proposta con la normativa UE esistente.....	
4.4. Le pratiche di AI vietate.....	
4.5. I divieti d'uso dell'AI: la valutazione dei sistemi ad alto rischio.....	
4.6. Le responsabilità .....	
4.7. Le sanzioni .....	
4.8. I 'punti di contatto con il GDPR' .....	
<b>5. Elaborazione dati e categorie speciali</b> .....	
5.1. Trattamento di categorie particolari di dati personali .....	
5.2. Rapporto pubblico-privato .....	
5.3. Rapporto privato-privato.....	
<b>Considerazioni conclusive</b> .....	
<b>Bibliografia</b> .....	
<b>Sitografia</b> .....	

## Considerazioni introduttive

La presente trattazione si prefigge l'obiettivo di esaminare i problemi giuridici sollevati dall'uso dell'intelligenza artificiale nell'ambito del trattamento dei dati, con particolare riguardo per i processi decisionali automatizzati. Essa fornisce un inquadramento approfondito della normativa europea e nazionale concernente il settore, nonché del materiale preparatorio del regolamento oggi noto come AI Act.

L'elaborato fornisce una ricostruzione generale dell'evoluzione dei sistemi di intelligenza artificiale dal punto di vista storico e, in misura approssimativa, tecnico, partendo dal celeberrimo test di Turing e concludendosi con una panoramica dei traguardi raggiunti dagli odierni sistemi di *machine learning*.

In primo luogo sono esaminati i problemi posti dall'IA dal punto di vista nozionistico: dagli anni Cinquanta al sopraccitato AI Act, non è infatti esistita una nozione universalmente accettata dei sistemi di intelligenza artificiale. Sono inoltre forniti spunti concernenti i rapporti fra il diritto e l'intelligenza artificiale, esaminando parte della vasta proliferazione di documenti concernenti principi volti a fornire una guida normativa in materia.

Segue una preliminare ricostruzione dell'evoluzione della disciplina europea e nazionale della privacy, esaminando in particolare il ruolo decisivo della Direttiva 95/46/CE del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. La normativa in questione ha infatti inciso sul quadro storico della disciplina del trattamento dei dati personali in Italia, poiché determinò l'adozione della l. n. 675 del 31 dicembre 1996, inerente alla tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.

La trattazione prosegue con un'analisi della normativa sulla tutela dei dati personali prevista dal Regolamento 2016/679, ossia il Regolamento generale sulla protezione dei dati, o "GDPR".

Sono esaminati in dettaglio i diritti del destinatario del trattamento e le caratteristiche del consenso, nonché le prerogative e gli obblighi del titolare e del responsabile del trattamento. È stata dedicata particolare attenzione ai requisiti e i principi del trattamento automatizzato, nonché il processo decisionale automatizzato e le ipotesi di intervento umano, focalizzandosi sull'uso di algoritmi di intelligenza artificiale.

L'elaborato tratta estensivamente il contenuto della proposta di regolamento pubblicata dalla Commissione europea in data 21 aprile 2021, concernente la prima potenziale legge volta a delineare un quadro normativo il settore dell'intelligenza artificiale. Saranno esaminati i benefici socioeconomici derivanti dall'uso di tali tecnologie, nonché i relativi pericoli; questi ultimi costituiscono il fondamento dell'approccio basato sul rischio suggerito nella proposta, che suddivide i sistemi di intelligenza artificiale in tre categorie, prevedendo, sulla base di criteri di sussidiarietà e proporzionalità, obblighi di trasparenza e adeguate procedure di valutazione di conformità.

Segue infine una breve analisi sull'elaborazione delle categorie particolari di dati personali, precedentemente noti come “dati sensibili”, fornendo una panoramica del quadro normativo oggi previsto dal Regolamento 2016/679 ed esempi di operazioni di trattamento svolte da enti statali o tra privati.

# CAPITOLO I

## Quadro generale dell'intelligenza artificiale

### 1.1 Nozione di intelligenza artificiale e machine learning

*“L'intelligenza artificiale è importante quanto la scoperta del fuoco e dell'elettricità.”*

Così l'amministratore delegato di Google, Sundar Pichai, ha definito il potenziale impatto dell'intelligenza artificiale sul futuro dell'umanità, enfatizzandone le potenzialità nel contesto della risoluzione di problemi di portata globale, quali il cambiamento climatico, nonché nel settore sanitario, come la cura del cancro.<sup>1</sup> Sebbene l'intelligenza artificiale sia ormai ampiamente diffusa in numerosi settori dell'odierno contesto socioeconomico, non esiste tuttora una definizione universalmente accettata per tale disciplina.<sup>2</sup> La Proposta di regolamento del parlamento europeo e del consiglio del 2021, di cui si tratterà estensivamente, ha fornito una nozione particolarmente attendibile, che costituirà la base della presente trattazione.

Prima di approfondire il tema dell'intelligenza artificiale, è opportuno definire in via preliminare in cosa consista l'intelligenza umana, formando questa il termine naturale di paragone nel contesto delle funzioni svolte dagli algoritmi. Come per le IA, la nozione è sfuggente, ma si può affermare che il concetto di intelligenza concerna le capacità cognitive dell'uomo; specificamente, la capacità di questi di individuare la soluzione corretta, o il processo più efficace per la risoluzione di un problema.<sup>3</sup> Rileva in tal senso la capacità dell'uomo di trarre informazioni dall'ambiente circostante attraverso i propri organi di senso, elaborandole in modo complesso. Ed è in questo campo che l'intelligenza artificiale è in grado di produrre risultati notevoli, sebbene in ogni caso sprovvista di caratteristiche quali la volontà o l'intelletto.

---

<sup>1</sup> CNN, Petroff. A., “Google CEO: AI is 'more profound than electricity or fire'”, 24 gennaio 2018, <https://money.cnn.com/2018/01/24/technology/sundar-pichai-google-ai-artificial-intelligence/index.html>

<sup>2</sup> Pizzetti F., *Intelligenza Artificiale, protezione dei dati personali e regolazione*, G. Giappichelli Editore, ed. 2018, p. 202

<sup>3</sup> Pizzetti F., *Intelligenza Artificiale, protezione dei dati personali e regolazione*, G. Giappichelli Editore, ed. 2018, p. 191

L'intelligenza artificiale è genericamente definibile come un insieme di algoritmi che, attraverso complesse funzioni logico-matematiche, cerca di ricreare l'intelligenza dell'uomo, con particolare riguardo alle capacità di apprendimento di quest'ultimo, facendo sì che la macchina, ripetendo determinate azioni più volte, apprenda dagli errori commessi e diventi sempre più efficiente. È possibile, pertanto, definire tentativamente l'IA come l'automazione di comportamenti intelligenti.<sup>4</sup>

Il documento informale di 17 pagine noto come 'proposta di Dartmouth', in occasione della proposta della Conferenza di Dartmouth ad opera di John McCarthy, Marvin Minsky, Nathaniel Rochester e Claude Shannon, definisce così l'intelligenza artificiale nel 1955: «*Lo studio procederà sulla base della congettura per cui, in linea di principio, ogni aspetto dell'apprendimento o una qualsiasi altra caratteristica dell'intelligenza possano essere descritte così precisamente da poter costruire una macchina che le simuli. Si tenterà di capire come le macchine possano utilizzare il linguaggio, formare astrazioni e concetti, risolvere tipi di problemi riservati per ora solo agli esseri umani e migliorare se stesse.*».<sup>5</sup>

I dizionari anglosassoni definiscono l'intelligenza artificiale come lo studio e lo sviluppo di sistemi computerizzati in grado di copiare i comportamenti intelligenti dell'uomo<sup>6</sup>; o, ancor più semplicisticamente, la scienza che permette ai computer di fare ciò che è in grado di fare l'uomo<sup>7</sup>. L'intelligenza artificiale è stata definita anche come l'abilità di una macchina di mostrare capacità umane quali il ragionamento, l'apprendimento, la pianificazione e la creatività<sup>8</sup>; nozione, questa, che solleva non poche questioni dal punto di vista etico.

---

<sup>4</sup> Nicotra M., Intelligenza artificiale, cos'è, come funziona e le applicazioni in Italia ed Europa,

<https://www.agendadigitale.eu/sicurezza/privacy/intelligenza-artificiale-la-via-delleuropa-su-regole-e-investimenti/>

<sup>5</sup> McCarthy, J., Minsky, M. L., Rochester, N., Shannon, C. E.. *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, 31 agosto 1955. *AI Magazine*, 27(4), 12, 2006. <https://doi.org/10.1609/aimag.v27i4.1904>

<sup>6</sup> Oxford Learner's Dictionaries, "Artificial intelligence",

<https://www.oxfordlearnersdictionaries.com/definition/english/artificial-intelligence>

<sup>7</sup> Cambridge Dictionary, "Artificial intelligence", <https://dictionary.cambridge.org/dictionary/english-italian/artificial-intelligence>

<sup>8</sup> Attualità Parlamento Europeo, *Che cos'è l'intelligenza artificiale e come viene usata?*, 3 settembre 2020, aggiornato il 29 marzo 2021, <https://www.europarl.europa.eu/news/it/headlines/society/20200827STO85804/che-cos-e-l-intelligenza-artificiale-e-come-viene-usata>

L'*High Level Group on Artificial Intelligence*, pannello indipendente istituito dalla Commissione Europea composto da 52 esperti del settore, ha elaborato una nozione attendibile. Con l'obiettivo di fornire linee guida volte ad affrontare le sfide nel medio e lungo termine poste dall'intelligenza artificiale, il Gruppo identifica questa come sistemi in grado di comportarsi in modo intelligente che, analizzando il proprio ambiente, compiono azioni con un certo livello di autonomia, conseguendo determinati obiettivi. Possono essere basati interamente su software, agendo dunque esclusivamente nel mondo virtuale, come avviene nel caso degli assistenti vocali o motori di ricerca; alternativamente possono essere incorporati in dispositivi hardware, come robot o automobili cosiddette *self-driving*.<sup>9</sup>

La proposta di regolamento del parlamento europeo e del consiglio del 2021<sup>10</sup>, concernente l'armonizzazione di regole nell'ambito dell'intelligenza artificiale, definisce infine l'IA come “una famiglia di tecnologie in rapida evoluzione in grado di apportare una vasta gamma di benefici economici e sociali in tutto lo spettro delle attività industriali e sociali”.

I moderni sistemi che fanno uso dell'intelligenza artificiale necessitano di notevoli quantità di dati al fine di realizzare il proprio potenziale; l'Autorità per la Protezione dei Dati Norvegese si è espressa sul punto, sostenendo che le IA necessitano di *huge volumes* di dati al fine di prendere decisioni intelligenti. Anche l'*UK Information Commissioner* ha sostenuto che l'intelligenza artificiale opera collezionando ed analizzando tutti i dati disponibili.<sup>11</sup>

Diversamente da quanto suggerito dalle opere di *science fiction*, dunque, l'intelligenza artificiale, per quanto sia oggi in grado di operare in sistemi autonomi e senza l'intervento dell'uomo, produrrà sempre risultati prevedibili: si è ben lontani da quanto suggerito da opere cinematografiche quali *Space Odyssey*, che figura una IA indipendente, emotiva e addirittura ostile all'uomo. In particolare, come precedentemente osservato in riferimento ai sistemi di

---

<sup>9</sup> High-Level Expert Group on Artificial Intelligence, *A definition of Artificial Intelligence: main capabilities and scientific disciplines*, Brussels, 18 dicembre 2018, [https://ec.europa.eu/futurium/en/system/files/ged/ai\\_hleg\\_definition\\_of\\_ai\\_18\\_december\\_1.pdf](https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf)

<sup>10</sup> *Proposta di regolamento del parlamento europeo e del consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione*, <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52021PC0206>

<sup>11</sup> Kuner C., Cate H. F., Lynskey O., Millard C., Loideain N. N., Svantesson D. J. B., “*Expanding the artificial intelligence-data protection debate*”, *International Data Privacy Law*, Volume 8, Issue 4, Novembre 2018, pp. 289–292, <https://doi.org/10.1093/idpl/ipy024>



intelligenza artificiale forte, ad oggi non esiste alcun sistema in grado di replicare in maniera indistinguibile la mente umana. In particolare, non può neppur dirsi che una macchina sia in grado di pensare; questa è contraddistinta da una notevole capacità computazionale, ma è limitata al mondo della logica ed ai modelli forniti in partenza dall'uomo; trattasi, dunque, di un agente logico incapace di contraddirsi.

Nella sua accezione più tecnica, l'intelligenza artificiale opera come un agente razionale privo di caratteristiche tipicamente umane, quali la volontà o l'intuito; essa agisce solo in base alla logica ed entro un numero prestabilito di possibilità a mezzo di algoritmi logico-matematici. L'agente misura le diverse configurazioni che possono essere assunte dal mondo con cui interagisce, limitatamente a quelle che è in grado di riconoscere sulla base dei modelli forniti dall'uomo in partenza. Analizzando i cambiamenti nell'ambiente che la circonda, la macchina raccoglie dati, che utilizza per risolvere problemi specifici a mezzo della propria potenza computazionale.<sup>12</sup>

È di fondamentale importanza osservare come il termine “intelligenza artificiale” sia ascrivibile a diverse tipologie della stessa; rilevano in tal senso i sistemi di “intelligenza artificiale debole”, o *narrow AI*, nonché “intelligenza artificiale forte”, o *strong AI*.

I sistemi di intelligenza artificiale debole sono impiegati per la risoluzione di problemi specifici e lo svolgimento di singole funzioni. In quanto tali, essi non godono della flessibilità dell'intelligenza umana, ma consentono di rimpiazzare e sorpassare l'uomo con risultati notevoli grazie alla propria elevata potenza di calcolo, che consente loro di analizzare migliaia di dati ad una velocità elevata.

---

<sup>12</sup> D'Acquisto G., *Intelligenza Artificiale – Elementi*, Giappichelli, 2021, p. 16

La caratteristica principale dell'intelligenza artificiale debole consiste, dunque, nella capacità di tali algoritmi di svolgere singole funzioni meglio dell'uomo, replicandone l'intelligenza in settori specifici.<sup>13</sup> Non si tratta di modelli in grado di deviare da quanto stabilito nella loro base di partenza: in altre parole, non sono in grado di imparare, contrariamente ai sistemi di *machine learning* e *deep learning*.

Seguono i sistemi di intelligenza artificiale forte, noti come *strong AI*, *full AI* o *artificial general intelligence (AGI)*. Trattasi in questo caso di forme di IA in grado di operare in maniera indistinguibile dall'uomo: in altre parole, simulano perfettamente la mente umana, condividendone la flessibilità, senza essere vincolate a funzioni o problemi specifici.<sup>14</sup> Si tratta di modelli attualmente ipotetici, ma in linea con l'obiettivo della scienza di creare sistemi in grado di replicare l'intelligenza umana.

A fronte degli avanzamenti tecnologici nei settori sopra delineati, è necessario definire il concetto di *machine learning*, noto in italiano come apprendimento automatico. Trattasi di un sottoinsieme della scienza dell'intelligenza artificiale che, individuando *pattern* nei dati raccolti dall'ambiente tramite sensori, è in grado di effettuare previsioni su dati futuri. Tali sistemi sono in grado di imparare e migliorare con l'esperienza, seppur non in modo paragonabile all'uomo, permettendo numerose applicazioni pratiche, da semplici giochi al settore automobilistico, nonché a tecniche avanzate di *photo* e *video editing*.<sup>15</sup>

Un altro recente esempio di tecnologia *machine learning* è il programma Google "MuZero", in grado di comprendere autonomamente le regole di giochi da tavola, quali gli scacchi, o giochi da tavola orientali, quali Go e Shogi, nonché videogiochi.<sup>16</sup>

---

<sup>13</sup> TechTarget, Labbe M., Wigmore I., "narrow AI (weak AI)", agg. giugno 2021, <https://www.techtarget.com/searchenterpriseai/definition/narrow-AI-weak-AI#:~:text=Narrow%20AI%2C%20also%20known%20as,intelligence%20for%20a%20dedicated%20purpose>

<sup>14</sup> Wirth N., *Hello marketing, what can artificial intelligence help you with?* International Journal of Market Research: the Journal of the Market Research Society /, 60(5), 2018, pp. 435–438. <https://doi.org/10.1177/1470785318776841>

<sup>15</sup> Meisner B., *What is the future of artificial intelligence in photo editing?*, 20 gennaio 2020, <https://www.forbes.com/sites/forbesbusinesscouncil/2022/01/20/what-is-the-future-of-artificial-intelligence-in-photo-editing/?sh=238192a7547c>

<sup>16</sup> BBC, *DeepMind's AI agent MuZero could turbocharge YouTube*, 23 dicembre 2020, <https://www.bbc.com/news/technology-55403473>

I sistemi di *machine learning* sfruttano, dunque, modelli matematici per l'elaborazione di dati ed estrazione di informazioni utili, effettuando poi previsioni su elementi sconosciuti, suggerendo quali azioni o decisioni prendere a mezzo di un procedimento automatizzato. I modelli di machine learning in questione sono addestrati, a mezzo di algoritmi di apprendimento, ad operare in circostanze specifiche: le relative configurazioni sono modificate in base a *training data*, o insiemi di addestramento.<sup>17</sup>

Sfruttando le capacità di apprendimento della macchina, questa è in grado di utilizzare le finalità di trattamento perseguite all'inizio della sua operatività come base di partenza e andare oltre, elaborandone di ulteriori e diverse, ma soprattutto non predeterminate.<sup>18</sup> È importante osservare come intelligenza artificiale e *machine learning* non siano la stessa cosa. Nei sistemi di *machine learning*, l'algoritmo apprende dai dati precedentemente raccolti, producendo un nuovo comportamento.

Questo è programmato per considerare unicamente specifiche variabili di ingresso e uscita dei fenomeni che osserva, elaborandone le relative leggi logico-matematiche. Divergono quindi dagli ordinari sistemi di intelligenza artificiale nell'accezione precedentemente fornita. I sistemi di *machine learning* sono in grado di "imparare"; non raggiungono però ancora il livello dell'intelletto umano, che è in grado di analizzare qualsiasi fenomeno, non sussistendo alcun limite in termini di input e output prestabiliti.

---

<sup>17</sup> Lindholm, A., Wahlström, N., Lindsten, F., & Schön, T. (2022). *Machine Learning: A First Course for Engineers and Scientists*. Cambridge: Cambridge University Press. doi:10.1017/9781108919371

<sup>18</sup> Anselmi N., Olivi G., *Machine learning, i problemi per la privacy (e le possibili soluzioni)*,

<https://www.agendadigitale.eu/cultura-digitale/machine-learning-i-problemi-per-la-privacy-e-le-possibili-soluzioni/>

## 1.2 Evoluzione dell'intelligenza artificiale

La concezione odierna di intelligenza artificiale trae senz'altro spunto dalla celebre opera *Runaround* di Isaac Asimov, scrittore di fantascienza che, nel 1942, elenca tre precetti che ricorreranno più volte nei suoi racconti; trattasi specificamente delle Tre leggi della robotica della collezione “*Io, Robot*”, cui obbediscono le macchine che figurano nelle opere dell'autore.

1. *«Un robot non può recar danno a un essere umano né può permettere che, a causa del suo mancato intervento, un essere umano riceva danno.*
2. *Un robot deve obbedire agli ordini impartiti dagli esseri umani, purché tali ordini non vadano in contrasto alla Prima Legge.*
3. *Un robot deve proteggere la propria esistenza, purché la salvaguardia di essa non contrasti con la Prima o con la Seconda Legge.»<sup>19</sup>*

Per quanto le opere di Asimov risalgano al secolo scorso, in un'epoca in cui gli strumenti *hardware* e *software* erano ben lontani dagli enormi progressi raggiunti dalla tecnologia odierna, è già possibile osservare l'attenzione rivolta alla componente etica inevitabilmente insita nell'utilizzazione di macchine pensanti nella società umana.

In particolare, Asimov pone particolare enfasi sull'incolumità dell'uomo, nonché all'obbedienza della macchina: esigenze, queste, di particolare rilevanza oggigiorno, se si considerano i tentativi di utilizzo dei sistemi di intelligenza artificiale nel contesto delle *self-driving cars*, ma anche in quello militare.

---

<sup>19</sup> Traduzione di Rambelli R. in *Io, Robot*, Bompiani, 1963.

Nel 1950 il matematico Alan Turing propone in un articolo<sup>20</sup> pubblicato sulla rivista *Mind* il celeberrimo esperimento noto come il “Test di Turing”, focalizzato sui risultati pratici che una macchina può produrre. Esso consiste in un gioco di imitazione che coinvolge tre partecipanti: un uomo, definito A; una donna, definita B; infine un terzo, definito C, che è separato dai primi due.

Quanto ai compiti affidati a ciascuno dei partecipanti, si chiede a C di determinare chi sia l'uomo e chi sia la donna a mezzo di una serie di domande; in particolare, B è incaricata di assistere C nel dedurre correttamente l'identità dei due partecipanti, mentre A deve indurre C ad effettuare un'identificazione errata. L'esperimento prevede la sostituzione di A, originariamente un partecipante umano, con una macchina.

Qui è insita la premessa del test di Turing: nell'ipotesi in cui la percentuale di successo di C nell'identificare chi sia l'uomo e chi la donna non vari quando A è una macchina, potrà affermarsi che questa abbia prodotto un pensiero; e poiché il risultato finale è identico a quello che sarebbe stato prodotto dal cogitare umano, la macchina è da considerarsi intelligente.

La disciplina dell'intelligenza artificiale nasce ufficialmente con la Conferenza di Dartmouth tenutasi nel 1956 nel Nempshire. L'evento viene proposto da John McCarthy, Marvin Minsky, Nathaniel Rochester e Claude Shannon nella già citata Proposta del 1955 inerente al *Dartmouth Summer Research Project on Artificial Intelligence (DSRPAI)*<sup>21</sup>, in occasione del quale il termine “*artificial intelligence*” sarà coniato per la prima volta. La conferenza sarà seguita da notevoli successi nel campo delle IA, in particolare con la realizzazione di programmi in grado di simulare una conversazione umana o risolvere problemi.

---

<sup>20</sup> Turing A., “*Computing Machinery and Intelligence*,” *Mind*, LIX/236, 1950, pp. 433-460.

<sup>21</sup> McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E.,. *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, Agosto 31, 1955. *AI Magazine*, 27(4), 12, 2006.  
<https://doi.org/10.1609/aimag.v27i4.1904>

Un esempio di notevole rilievo nell'ambito della simulazione del dialogo umano è il programma ELIZA, ideato da Joseph Weizenbaum al MIT Artificial Intelligence Laboratory 10 anni dopo la Conferenza di Dartmouth, tra il 1964 e il 1966<sup>22</sup>. Diversamente dal test di Turing, questo prevede la partecipazione di un solo interrogatore umano ed una macchina, in questo caso un programma dialogico automatizzato in grado di apprendere dalle risposte che riceve. In tal modo, ELIZA era in grado di simulare il dialogo di un essere umano<sup>23</sup>.

Ulteriori sviluppi nella disciplina dell'intelligenza artificiale portarono alla realizzazione del General Problem Solver da parte di Herbert Simon, Cliff Shaw e Allen Newell. Trattasi un programma in grado di risolvere semplici problemi: specificamente, come nel caso di ELIZA, di un sistema esperto, ossia un insieme di regole operanti in base alla premessa che l'intelletto umano operi secondo funzioni *if-then*; in quanto tale, esso è in grado di operare unicamente in ambiti circoscritti<sup>24</sup>. Algoritmi, dunque, ben lontani dai moderni sistemi di *machine learning* e *deep learning*, che mostrano una amplissima flessibilità, consentendo loro di riconoscere volti umani ed apprendere in misura simile a quella di un bambino<sup>25</sup>.

Nonostante gli sforzi profusi a partire dagli anni '40 nell'ambito della ricerca su reti neurali artificiali, nel 1969 Marvin Minsky e Seymour Papert dimostrarono che lo sviluppo di sistemi di IA più avanzati era limitato dalla potenza computazionale delle componenti hardware esistenti all'epoca, portando ad un ristagno dei progressi nel settore.<sup>26</sup> In particolare, Minsky affermò nel 1967 che le problematiche in questione sarebbero state “sostanzialmente risolte” nel corso di una generazione.<sup>27</sup>

---

<sup>22</sup> D'Acquisto G., *Intelligenza Artificiale – Elementi*, Giappichelli, 2021, p. 4

<sup>23</sup> Weizenbaum J., *Computer Power and Human Reason: From Judgment to Calculation*. New York: W. H. Freeman and Company.

<sup>24</sup> Haenlein, & Kaplan, A., *A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence*. *California Management Review*., 61(4), 2019, p. 3, <https://doi.org/10.1177/0008125619864925>

<sup>25</sup> Hutson M., “How Researchers Are Teaching AI to Learn Like a Child,” *Science*, 24 maggio, 2018, <https://www.sciencemag.org/news/2018/05/how-researchers-are-teaching-ai-learn-child>

<sup>26</sup> Haenlein, & Kaplan, A., *A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence*. *California Management Review*., 61(4), 2019, p. 8, <https://doi.org/10.1177/0008125619864925>

<sup>27</sup> Strickland E., *The turbulent past and future of artificial intelligence*, 30 settembre 2021, <https://spectrum.ieee.org/history-of-ai>

L'evoluzione dell'intelligenza artificiale fu costellata nel periodo che seguì da diversi successi nel campo di giochi da tavolo. Nel 1989 ebbe inizio presso IBM lo sviluppo di *Deep Blue*, una macchina in grado di giocare a scacchi: trattavasi di un sistema esperto installato su un supercomputer *ad hoc*. Grazie alla sua capacità di valutare e ponderare 100 milioni di possibili mosse al secondo, nel 1997 *Deep Blue* diverrà la prima macchina in grado di vincere una partita contro il campione mondiale Garry Kimovich Kasparov.<sup>28</sup>

A partire dal 2010 l'intelligenza artificiale è soggetta ad un nuovo boom. È innanzitutto divenuto possibile accedere a notevoli quantità di dati, anche grazie a sistemi quali Google. Inoltre, in seguito ai notevoli progressi nel campo delle componenti hardware, in particolare le schede video normalmente destinate a scopo videoludico, in grado di effettuare oltre mille miliardi di transazioni al secondo, è divenuto possibile migliorare esponenzialmente l'addestramento dei modelli per l'apprendimento automatico.<sup>29</sup> Nel 2011 una nuova AI di IBM, Watson, sconfigge i campioni del gioco *Jeopardy!*, ove il partecipante, data la risposta, deve indovinare la domanda.<sup>30</sup>

Nel 2015 fu raggiunto un nuovo traguardo quando il programma Google AlphaGo, sviluppato dai laboratori di Deep Mind, utilizzando il già citato sistema di *deep learning* e in seguito ad un addestramento basato su 30 milioni di mosse utilizzate da giocatori esperti, batté il campione mondiale del gioco da tavolo Go<sup>31</sup>, considerevolmente più complesso degli scacchi.

Il test di Turing di cui si è precedentemente discusso è ancora utilizzato come parametro di riferimento per determinare qualora una macchina sia intelligente o meno; traguardo, questo, che alcuni ritengono essere stato raggiunto nel 2014. In occasione del sessantesimo anniversario della morte di Turing, il chatbot Eugene Goostman, programmato per simulare

---

<sup>28</sup> Goodrich J., IEEE Spectrum, *How IBM's Deep Blue Beat World Champion Chess Player Garry Kasparov The supercomputer could explore up to 200 million possible chess positions per second with its AI program*, <https://spectrum.ieee.org/how-ibms-deep-blue-beat-world-champion-chess-player-garry-kasparov>

<sup>29</sup> Benanti P., *Human in the Loop*, Mondadori, giugno 2022, p. 64

<sup>30</sup> Benanti P., *Human in the Loop*, Mondadori, giugno 2022, p. 65

<sup>31</sup> BBC, *Artificial intelligence: Google's AlphaGo beats Go master Lee Se-dol*, 26 marzo 2016, <https://www.bbc.com/news/technology-35785875>

una conversazione con un ragazzo ucraino di 13 anni, è stato in grado di ingannare il 33% dei giudici partecipanti.<sup>32</sup>

Gli ultimi sviluppi dei sistemi di *machine learning* hanno condotto al paradigma del cosiddetto *deep learning*: attraverso modalità avanzate di elaborazione dei dati, l'agente è in grado di produrre risultati sempre più simili a quelli normalmente attribuiti all'astrazione dell'uomo. Come precedentemente accennato, l'intelligenza artificiale necessita di grandi quantità di dati per produrre risultati precisi: le reti neurali sono pertanto in grado di sfruttarle in modo sempre più efficiente, grazie all'elevata capacità computazionale delle macchine odierne<sup>33</sup>.

Parte integrante del paradigma del *deep learning* sono le reti neurali artificiali, definibili come modelli computazionali ed approssimatori universali applicabili ad una grande varietà di problemi<sup>34</sup>; specificamente, trattasi di modelli matematici che simulano il funzionamento del cervello umano; i relativi algoritmi agiscono, dunque, come veri e propri neuroni artificiali. Tali reti sono utilizzate per risolvere problemi inerenti ad ambiti come l'informatica, l'elettronica, la simulazione o altre discipline,<sup>35</sup> e sono da considerarsi la frontiera del settore delle IA.

---

<sup>32</sup> "News Makers." 2014. Maclean's 127 (24): 10.

<https://search.ebscohost.com/login.aspx?direct=true&db=bsu&AN=96454285&site=ehost-live>

<sup>33</sup> D'Acquisto G., *Intelligenza Artificiale – Elementi*, Giappichelli, settembre 2021, p. 183

<sup>34</sup> Khashei, Mehdi, Bijari M., "An Artificial Neural Network ( P, D, Q) Model for Timeseries Forecasting." *Expert systems with applications* 37.1 (2010), pp. 479–489. Web.

<sup>35</sup> N. Boldrini, *Reti neurali: cosa sono e a cosa servono*, 23 aprile 2022, <https://www.ai4business.it/intelligenza-artificiale/deep-learning/reti-neurali/>



### 1.3 I profili etici dell'intelligenza artificiale

L'intelligenza artificiale, tecnologia chiave applicata trasversalmente in molteplici e svariati settori e di rilevante importanza anche di carattere strategico e geopolitico, quali la sicurezza nazionale e internazionale, nonché la competitività economica e la supremazia tecnologica, presenta prospettive di sviluppi ancora non completamente definiti. In quanto tale è fonte di incertezze e solleva diverse problematiche di natura giuridica, ma anche etica<sup>36</sup>.

Rileva innanzitutto la questione degli ambiti, fino a poco tempo fa di esclusivo appannaggio dell'intervento umano, quali azione, supervisione e controllo, in cui le tecnologie IA possono operare, nonché i requisiti normativi e progettuali cui devono rispondere i sistemi ed applicazioni di IA per garantirne la tracciabilità e qualità. Un tema importante ai fini della presente trattazione è anche quello della responsabilità; in particolare, qualora questa ricada sull'operatore o il costruttore del sistema nell'ipotesi in cui si verificano effetti indesiderati.

Come si è evidenziato, i sistemi di IA e i progressi nel campo della tecnologia consentono di raccogliere e gestire grandi quantità di dati; l'automazione delle macchine rende poi possibili forme di sorveglianza di massa, volte alla lotta alla criminalità e a garanzia della sicurezza pubblica e nazionale, come però anche tentativi di manipolazione o influenza dell'esito di un processo democratico. I rapidi cambiamenti della società digitale introdotti dalle nuove tecnologie come l'IA, l'apprendimento automatico, la robotica e la rete Internet sollevano importanti questioni di ampio rilievo dal punto di vista etico su temi quali la privacy, la protezione dei dati, il modo in cui i diritti umani sono interessati dall'uso estensivo e intensivo dei dati a fini analitici e dalle nuove applicazioni tecnologiche.

L'applicazione delle innovazioni tecnologiche nel campo dell'intelligenza artificiale, infatti, come può già evincersi dall'analisi dell'evoluzione dell'intelligenza artificiale negli anni, oltre ad avere effetti positivi sulla società in termini di miglioramento ed ottimizzazione dei

---

<sup>36</sup> Confederazione Svizzera - Dipartimento Federale degli Affari Esteri, *"Intelligenza artificiale e regolamentazione internazionale – Rapporto all'attenzione del Consiglio Federale"*, 2022, p. 3 - <https://www.news.admin.ch/news/message/attachments/71098.pdf>

processi attraverso l'automazione, può produrre risultati indesiderati, sia in termini materiali, come danni a cose o persone (anche in termini di vite umane), sia in termini immateriali, come violazioni della privacy, nonché limitazioni della libertà personale, della libertà di espressione, discriminazione. Si crea da questo punto di vista un senso di incertezza sul rapporto tra IA e uomo. L'espansione della sfera digitale, con il sempre crescente trasferimento di attività dal contesto fisico al contesto digitale, è una tendenza inequivocabile della nostra società.

Con particolare riguardo alla tutela della privacy, la tecnologia IA, aumentando le potenzialità di raccolta ed analisi dei dati, funge da catalizzatore ed acceleratore di questo processo, innescando a sua volta ulteriori preoccupazioni. Le applicazioni di IA consentono, ad esempio, attività di sorveglianza generalizzata con analisi automatizzata dei video registrati<sup>37</sup> rispetto alla tradizionale modalità di sorveglianza specifica, commercializzazione dei dati personali che vengono resi disponibili - più o meno inconsapevolmente - ogni qualvolta si aderisce ad un servizio offerto senza costi.

Il dibattito etico sull'utilizzo delle innovazioni in questione non si discosta da quanto già suggerito dalle leggi sulla robotica di Asimov: le innovazioni tecnologiche devono essere orientate verso il bene comune. Si discute in tal senso di etica degli algoritmi, o "algoritica", al fine di orientare la *governance* (ossia il "modo di organizzare e amministrare territori e popolazioni") delle intelligenze artificiali, specie con riguardo al rispetto dei diritti di uguaglianza e di ricerca della propria felicità.

Partendo dal presupposto che lo scopo della riflessione etica è quello di rendere presente "la domanda critica sul senso dell'umano che l'innovazione tecnologica media" e "le modalità che possono garantire uno sviluppo umano autentico",<sup>38</sup> l'utilizzo delle IA, sarebbe lecito soltanto nella misura in cui i diritti sopraccitati siano rispettati. Si presenta inevitabilmente

---

<sup>37</sup> Choi Q. C., *Protecting Privacy in Surveillance Video While Mining It for Data: A new technique may help defend privacy while permitting useful analysis of surveillance data*, 19 aprile 2022, <https://spectrum.ieee.org/surveillance-privacy#toggle-gdpr>

<sup>38</sup> Benanti P., *Human in the Loop*, Mondadori, giugno 2022, pp. 128-130

l'esigenza di fare in modo che i progressi delle tecnologie garantiscano l'elaborazione di norme e strumenti entro i principi alla base della società democratica.

Gli attori incaricati dello sviluppo del quadro giuridico e degli strumenti necessari per un utilizzo dell'intelligenza artificiale lecito ed etico devono pertanto interrogarsi su numerose questioni nel contesto della valutazione degli effetti che possono derivare da una *mass-surveillance* automatizzata.

Occorre determinare qualora l'intelligenza artificiale sia applicata in modo proporzionale e trasparente (in termini di documentazione pubblica), nonché sull'eventuale esistenza di alternative meno invasive, potendo tali sistemi incidere sui diritti umani e le libertà dell'uomo in modo significativo, necessitando in quanto tali di adeguati strumenti di verifica e tutela.

Si presentano inoltre esigenze inerenti alla *cybersecurity* e al trattamento dei dati personali, con particolare riguardo per il consenso informato circa l'esistenza di tali sistemi e il modo in cui i dati in questione vengono utilizzati.<sup>39</sup> Temi, questi, di particolare rilevanza per la presente trattazione, in quanto il Regolamento generale sulla protezione dei dati (in inglese GDPR, ossia *General Data Protection Regulation*) include norme specificamente concernenti il trattamento automatizzato dei dati, seppur non con specifico riferimento all'intelligenza artificiale come intesa anni dopo nella Proposta del parlamento europeo.

L'utilizzo dei sistemi di intelligenza artificiale si estende anche nel settore dei sistemi giudiziari: nel 2018 la Commissione europea per l'efficacia della giustizia (CEPEJ) del Consiglio d'Europa ha emanato la Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi.

---

<sup>39</sup> Benanti P., *Human in the Loop*, Mondadori, giugno 2022, p. 132

Segue una succinta esposizione dei cinque principi da essa proposti.<sup>40</sup>

1. *Principio del rispetto dei diritti fondamentali: assicurare che l'elaborazione e l'attuazione di strumenti e servizi di intelligenza artificiale siano compatibili con i diritti fondamentali.*
2. *Principio di non-discriminazione: prevenire specificamente lo sviluppo o l'intensificazione di discriminazioni tra persone o gruppi di persone.*
3. *Principio di qualità e sicurezza: in ordine al trattamento di decisioni e dati giudiziari, utilizzare fonti certificate e dati intangibili con modelli elaborati multidisciplinariamente, in un ambiente tecnologico sicuro.*
4. *Principio di trasparenza, imparzialità ed equità: rendere le metodologie di trattamento dei dati accessibili e comprensibili, autorizzare verifiche esterne.*
5. *Principio del controllo da parte dell'utilizzatore: precludere un approccio prescrittivo e assicurare che gli utilizzatori siano attori informati e abbiano il controllo delle loro scelte.*

L'aspetto etico dell'Intelligenza Artificiale può anche essere esaminato da una duplice prospettiva: l'etica dell'Intelligenza Artificiale intesa come l'insieme di principi, linee guida, regole, normative che sono correlate con l'intelligenza Artificiale, e l'Intelligenza Artificiale "Etica" intesa come una Intelligenza Artificiale che si comporta secondo principi etici<sup>41</sup>.

Oltre alla problematica della raccolta di dati personali celata dietro applicazioni di uso comune, quali ad esempio le tecniche di riconoscimento facciale nel materiale multimediale (foto, video) condiviso sui "social", il riconoscimento con impronta digitale, la diffusione di elettronica di consumo "smart" (telefoni, televisori, elettrodomestici), *l'internet delle cose*, si

---

<sup>40</sup> Commissione europea per l'efficienza della giustizia, *Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi*, Introduzione, 3 dicembre 2018, p. 5, <https://rm.coe.int/carta-etica-europea-sull-utilizzo-dell-intelligenza-artificiale-nei-si/1680993348>

<sup>41</sup> Keng S., Weiyu W., *Artificial Intelligence (AI) Ethics: Ethics of AI and Ethical AI*, marzo 2020: <https://www.researchgate.net/publication/340115931>

pone l'ulteriore problema della difficoltà a riconoscere e tracciare chi è legalmente responsabile del trattamento di questi dati.

Le aziende tecnologiche fanno talvolta uso di *dark patterns*, intesi come interfacce ed esperienze utente implementate su piattaforme di social media, che portano chi le utilizza a prendere decisioni involontarie, riluttanti e potenzialmente dannose in merito al trattamento dei propri dati personali<sup>42</sup>, sollevando evidenti questioni etiche per quanto concerne l'utilizzo di IA in tali settori.

Il fatto stesso che un sistema IA sia progettato in modo da emulare o sostituire l'intelligenza umana solleva preoccupazioni sulla possibilità di introdurre meccanismi ingannevoli, pregiudizi ed errori cognitivi. Diversi studi hanno dimostrato che se non sono progettati ed implementati correttamente, le IA possono rispecchiare le convinzioni, talvolta inconsapevoli, di chi li ha creati; ed oltre ad acquisire i pregiudizi dai programmatori, le macchine in questione possono svilupparne anche in maniera del tutto autonoma<sup>43</sup>.

Si rivela dunque necessario assicurare che quanto più si sostituisce il livello di controllo aumentando l'autonomia della macchina, tanto più è necessario che la stessa si comporti "eticamente".

L'evoluzione ed il sempre più diffuso utilizzo dell'Intelligenza Artificiale ha stimolato da tempo un nutrito dibattito internazionale, in particolare sul piano della produzione di normative e regolamenti, di cui si parlerà più approfonditamente nel successivo §1.4.

---

<sup>42</sup> Mathur A., Acar G., Friedman J. M., Lucherini E., Mayer J., Chetty M., Narayanan A., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*. *Proc. ACM Hum. - Comput. Interact.* 3, CSCW, Article 81, novembre 2019, <https://doi.org/10.1145/3359183>

<sup>43</sup> Benanti P., "Le AI come uomini: intuitive ma con pregiudizi", 10 settembre 2018, <https://www.paolobenanti.com/post/2018/09/09/ai-pregiudizi>

Nel quadro della vastissima proliferazione di documenti di "principi" volti a fornire una guida normativa sui sistemi basati sull'IA, uno studio prodotto dall'Università di Harvard<sup>44</sup> ha analizzato i contenuti di trentasei importanti documenti sui principi etici dell'IA individuando in essi le più frequenti ricorrenze tematiche. Lo studio ha pertanto identificato otto temi maggiormente ricorrenti:

1. *Privacy (presente nel 97% dei documenti analizzati);*
2. *Responsabilità (97%);*
3. *Sicurezza e protezione (81%);*
4. *Trasparenza e spiegabilità (94%);*
5. *Equità e non-discriminazione (100%);*
6. *Controllo umano della tecnologia (69%);*
7. *Responsabilità professionale (78%);*
8. *Promozione dei valori umani (69%).*

Una seconda importante conclusione dello studio è che i documenti più recenti tendono a coprire tutti e otto questi temi; questo suggerisce che la discussione sui principi etici dell'IA sta iniziando a convergere, almeno tra le comunità responsabili dello sviluppo di questi documenti. Pertanto, questi temi possono rappresentare il "nucleo normativo" di un approccio basato sui principi all'etica e alla governance dell'IA.

---

<sup>44</sup> Fjeld, Jessica and Achten, Nele and Hilligoss, Hannah and Nagy, Adam and Srikumar, Madhulika, *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI*, , Berkman Klein Center Research Publication No. 2020-1, 15 gennaio 2020, <http://dx.doi.org/10.2139/ssrn.3518482>

## 1.4 Rapporti fra il diritto e l'intelligenza artificiale

### 1.4.1. Problematiche per la definizione di una regolamentazione della IA

Parallelamente alla evoluzione sopra delineata dei sistemi IA, i quali sono sempre più complessi e pervasivi in sempre nuovi settori della nostra vita quotidiana, si è sviluppato il dibattito e le attività finalizzate alla definizione di un quadro normativo e regolamentare per l'Intelligenza Artificiale, di cui si tratterà estensivamente nel contesto del GDPR e della Proposta di Regolamento UE.

La definizione di una regolamentazione della IA, in quanto tecnologia innovativa e in rapidissima evoluzione, richiede di affrontare e risolvere diversi problemi. Il primo problema è costituito dalla diversa velocità di evoluzione tra il diritto e la tecnologia. La seconda si sviluppa e cambia in modo esponenziale, ma i sistemi sociali, economici e legali cambiano in modo incrementale, e questo sta diventando un principio inevitabile nella vita moderna.<sup>45</sup> Il secondo problema è costituito dal dilemma di Collingridge<sup>46</sup>: quanto più una innovazione o cambiamento si sviluppa, tanto più si riducono i margini di intervento per apportare eventuali modifiche e aumenta, nel tempo, l'attenzione e la potenziale frustrazione dei suoi utenti; in altre parole, *“è difficile prevedere le implicazioni di una tecnologia finché non verrà adottata ed implementata in modo estensivo. Una volta raggiunto questo punto nel tempo, è difficile controllarne e cambiarne le implicazioni una volta che queste si sono radicate”*<sup>47</sup>.

Le conseguenze sociali di una tecnologia non possono essere previste all'inizio della vita della tecnologia; quando si scoprono conseguenze indesiderabili, tuttavia, la tecnologia è

---

<sup>45</sup> Dowson, L. *“The law of disruption occupies Wall Street”*, 16 ottobre 2011,

<https://www.forbes.com/sites/larrydownes/2011/10/16/the-law-of-disruption-occupies-wall-street/?sh=3468b3ef4ebb>

<sup>46</sup> Genus, & Stirling, A., *“Collingridge and the dilemma of control: Towards responsible and accountable innovation. Research Policy”*, 47(1), pp. 61–69, 2018, <https://doi.org/10.1016/j.respol.2017.09.012>

<sup>47</sup> Privacy Network, Nannini, L., *“Possibili Rischi per la Strategia Italiana sull'Intelligenza Artificiale a Confronto con l'EU AI Act”*, 2021, p. 9 [https://www.privacy-network.it/wp-content/uploads/2021/12/Regolamentazioni\\_AI\\_in\\_ITA\\_EU-7.pdf](https://www.privacy-network.it/wp-content/uploads/2021/12/Regolamentazioni_AI_in_ITA_EU-7.pdf)

spesso talmente parte dell'intero tessuto economico e sociale che il suo controllo è estremamente difficile.

#### **1.4.2. Ricognizione delle attività internazionale di regolamentazione della IA**

Nel panorama normativo internazionale relativo alla Intelligenza Artificiale attualmente in elaborazione, il Dipartimento federale della Confederazione Svizzera suggerisce in un rapporto del 2022 la possibilità di identificare seguenti cinque livelli<sup>48</sup>:

1. Diritto internazionale generale e trattati (organizzazioni dell'ONU, CCW, UNESCO).
2. Soft Law (G7, G20, OCSE).
3. Provvedimenti di Stati o Organizzazioni internazionali che hanno *de facto* rilevanza internazionale (USA, CINA, UE).
4. Autoregolamentazione sulla base di principi etici e norme tecniche da parte di aziende tecnologiche ed altri attori pubblici e privati (IEC, ISO, ITU, IEEE).
5. Normatività dei fatti sulla scorta dello sviluppo tecnologico.

Segue una panoramica delle attività di regolamentazione di produzione normativa sulla IA svolta ai vari livelli.

#### **Primo livello: Organismi internazionali**

Nel 2015, l'UNICRI (United Nations Interregional Crime and Justice Research Institute) ha lanciato il suo programma per l'IA e la Robotica e, con il supporto del Comune dell'Aia e del Ministero degli Affari Esteri dei Paesi Bassi, ha firmato l'accordo del paese ospitante per l'apertura (settembre 2017) del suo Centro per l'Intelligenza Artificiale e la Robotica a L'Aia, Paesi Bassi.

Questo centro è dedicato alla comprensione e alla gestione dei rischi e dei benefici dell'intelligenza artificiale e della robotica dal punto di vista della criminalità e della

---

<sup>48</sup> Confederazione Svizzera, Dipartimento Federale degli Affari Esteri, “*Intelligenza artificiale e regolamentazione internazionale – Rapporto all’attenzione del Consiglio Federale*”, 13 aprile 2022, § 5.2, <https://www.newsd.admin.ch/newsd/message/attachments/71098.pdf>



sicurezza attraverso la “*sensibilizzazione, l'educazione, lo scambio di informazioni e l'armonizzazione delle parti interessate*”.

A tal fine, l'UNICRI ha sviluppato un'ampia rete internazionale di soggetti con i quali collabora, tra cui l'Organizzazione internazionale della polizia criminale (INTERPOL), l'Unione internazionale delle telecomunicazioni (ITU), l'Istituto di ingegneria elettrica ed elettronica (IEEE), la Fondazione per Responsible Robotics, il World Economic Forum e il Center for Future Intelligence (CFI)<sup>49</sup>.

Istituito nel 2019 dal Consiglio d'Europa, il CAHAI (Comitato ad hoc sull'intelligenza artificiale) nasce con l'obiettivo di valutare la potenziale stesura di un quadro giuridico inerente all'applicazione delle IA, mantenendo i principi cardine inerenti ai diritti umani, la democrazia ed il principio di legalità.<sup>50</sup>

Nell'ambito dei lavori della CCW (Convenzione sulla Proibizione o Restrizione dell'uso di certe armi convenzionali, adottata nel 1980 ed entrata in vigore nel 1983, ratificata nella sua interezza dall'Italia), nel corso degli ultimi anni è stato affrontato specificatamente il problema delle tecnologie emergenti nell'area delle LAWS (Lethal Autonomous Weapons System), “*cosidetti ‘Killer Robots’*”<sup>51</sup>.

La Prima Commissione dell'Assemblea Generale dell'ONU<sup>5253</sup> “*esamina tutte le questioni relative al disarmo e alla sicurezza internazionale ed elabora, negozia ed approva tutti i testi delle risoluzioni sulla materia che saranno successivamente sottoposti all'Assemblea Generale per la loro adozione definitiva. A essa riferisce anche la Conferenza del Disarmo*

---

<sup>49</sup> United Nations Interregional Crime and Justice Research Institute, *Centre on Artificial Intelligence and Robotics*, [http://www.unicri.it/topics/ai\\_robotics/centre](http://www.unicri.it/topics/ai_robotics/centre)

<sup>50</sup> Consiglio d'Europa, *Ad Hoc Committee on Artificial intelligence*, 11 settembre 2019, [https://search.coe.int/cm/Pages/result\\_details.aspx?ObjectId=09000016809737a1](https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016809737a1)

<sup>51</sup> Rappresentanza Permanente d'Italia ONU – Ginevra, *La Convenzione su certe armi convenzionali e Protocolli annessi*, <https://italiarappginevra.esteri.it/rappginevra/it/il-disarmo/trattati-e-convenzioni/armi-conv-effetti-indiscriminati.html>

<sup>52</sup> General Assembly of the United Nations, *Disarmament and International Security (First Committee)*, <http://www.un.org/en/ga/first/>

<sup>53</sup> Rappresentanza Permanente d'Italia ONU – Ginevra, *La Prima Commissione dell'Assemblea Generale dell'ONU*, <https://italiarappginevra.esteri.it/rappginevra/it/il-disarmo/la-prima-commissione-dell-assemblea/>

*tramite un rapporto annuale che esamina ed è incaricata di approvare, prima dell'adozione da parte della Assemblea Generale”.*

Nell'ottobre 2017, le Nazioni Unite hanno tenuto una riunione congiunta del Consiglio economico e sociale delle Nazioni Unite (ECOSOC) ed il Comitato Economico e Finanziario (Secondo Comitato) per “*considerare il ruolo e l'impatto dell'intelligenza artificiale sullo sviluppo sostenibile*”<sup>54</sup>.

Nel 2017, due documenti presentati al Consiglio delle Nazioni Unite per i Diritti Umani (UNHRC) hanno discusso le implicazioni dell'utilizzo delle tecnologie dell'IA sui diritti umani<sup>55</sup>. L'analisi delle interrelazioni tra i diritti umani e l'Intelligenza Artificiale si è incentrata principalmente sulla significativa riduzione dell'impiego dell'intervento umano in vari settori a causa dell'automazione, lo sviluppo di sistemi di armi letali autonomi, l'impatto sulla privacy del software di riconoscimento facciale, i rischi di discriminazione attraverso la replica o l'esacerbazione dei pregiudizi nei sistemi di intelligenza artificiale e gli effetti di alcuni metodi di "polizia predittiva".

## **Secondo livello: Soft Law**

Il campo della Robotica e dell'IA è un ambito al quale sembra adattarsi la flessibilità della *soft law*, che, non essendo vincolante e dunque inerentemente più flessibile rispetto alle ordinarie forme di regolamentazione, meglio riesce a stare al passo con la natura dinamica dei processi tecnologici<sup>56</sup>.

L'OCSE (Organizzazione per la Cooperazione e lo Sviluppo Economico) ha pubblicato nel 2019 la “*Recommendation of the Council on Artificial Intelligence*”. Questa mira a

---

<sup>54</sup> United Nations Sustainable Development Blog, “*The Future of Everything – Sustainable Development in the Age of Rapid Technological Change*”, 9 ottobre 2017, <https://www.un.org/sustainabledevelopment/blog/2017/10/looking-to-future-un-to-consider-how-artificial-intelligence-could-help-achieve-economic-growth-and-reduce-inequalities/>

<sup>55</sup> Cullen D., *Why Artificial Intelligence Is Already a Human Rights Issue*, Oxford Human Rights Hub, 31 dicembre 2018, <http://ohrh.law.ox.ac.uk/why-artificial-intelligence-is-already-a-human-rights-issue/>,

<sup>56</sup> Chiarelli M., *La sfida della regolazione europea dell'intelligenza artificiale*, 20 dicembre 2019, <https://www.diritto.it/la-sfida-della-regolazione-europea-dellintelligenza-artificiale/>

promuovere l'innovazione e la fiducia nel campo dell'intelligenza artificiale, gestendola in modo affidabile ed assicurando simultaneamente il rispetto dei diritti umani e dei valori democratici.

A complemento degli standard OCSE esistenti in settori quali privacy, gestione dei rischi per la sicurezza digitale e condotta aziendale responsabile, la Raccomandazione si concentra su questioni specifiche del settore, individuando cinque principi complementari basati su valori per una gestione responsabile di una intelligenza artificiale affidabile e invita gli attori dell'IA a promuoverle e attuarle. Seguono i principi in questione:

- *“Crescita inclusiva, sviluppo sostenibile e benessere;*
- *Valori incentrati sull'uomo e la correttezza;*
- *Trasparenza;*
- *Robustezza e sicurezza;*
- *Responsabilizzazione.”*

Coerentemente con questi principi, la Raccomandazione include anche cinque raccomandazioni ai decisori politici riguardanti le politiche nazionali e la cooperazione internazionale per una IA affidabile, vale a dire:

- *Investire nella ricerca e nello sviluppo dell'IA;*
- *Promuovere un ecosistema digitale per l'IA;*
- *Modellare un ambiente politico favorevole all'IA;*
- *Costruire capacità umane e prepararsi alla trasformazione del mercato del lavoro;*
- *La cooperazione internazionale per una IA affidabile.*<sup>57</sup>

Nel giugno 2020 il G7 ha avviato la GPAI (*Global Partnership on Artificial Intelligence*)<sup>58</sup>, e nel giugno 2019, il G20 ha adottato i principi dell'IA incentrata sull'uomo, che si ispirano ai principi dell'IA dell'OCSE.

---

<sup>57</sup> OECD, *Recommendation of the Council on Artificial Intelligence*, 22 maggio 2019, <https://oecd.ai/en/assets/files/OECD-LEGAL-0449-en.pdf>

<sup>58</sup> GPAI – The Global partnership on Artificial Intelligence, <https://gpai.ai/about/>

### **Terzo livello: Stati o Organizzazioni internazionali che hanno *de facto* rilevanza internazionale**

Nel contesto di una più ampia strategia politico-economica per lo sviluppo delle tecnologie AI, l'amministrazione USA ha emanato il 17 novembre 2020 una *Guidance for Regulation of Artificial Intelligence Application* contenente un decalogo di principi a cui tutte le agenzie federali dovranno attenersi allorché si trovino a regolamentare lo sviluppo, la vendita e l'utilizzo della IA, intese nell'accezione "debole" di cui si è trattato<sup>59</sup>. L'intento primario di questo insieme di principi è quello di rimuovere gli ostacoli all'innovazione e alla crescita dell'AI nel settore privato.

Gli USA premono sulla UE affinché recepisca il principio di flessibilità regolamentare, nel timore che l'Unione imponga un quadro normativo unico e troppo pesante, limitando lo sviluppo e la commercializzazione delle tecnologie AI a fronte delle preoccupazioni etiche che queste destano in tema di controllo governativo, privacy, sicurezza informatica e futuro del lavoro. Ciò al fine di evitare che l'introduzione di vincoli eccessivi penalizzi la competitività dei paesi occidentali (su tutte, la leadership tecnologica americana) rispetto a nazioni terze (su tutte, la Cina) che non sembrano avere remore in tema di utilizzo esteso e intensivo dell'intelligenza artificiale<sup>60</sup>.

La Cina nel 2017 ha emanato un piano strategico di sviluppo rispetto all'IA "*The Next Generation Artificial Intelligence Development Plan*", con lo scopo di definire gli obiettivi strategici e le misure per il supporto dello sviluppo di dell'IA entro il 2030.<sup>61</sup>

---

<sup>59</sup> Office of Management & Budget, Exec. Office of the President, 17 novembre 2020, "*Guidance for Regulation of Artificial Intelligence Applications*", <https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf>

<sup>60</sup> Privacy.it, *Gli USA pressano la UE: no a normazione rigida su intelligenza artificiale*, 8 gennaio 2020, <https://www.privacy.it/2020/01/08/usa-normazione-intelligenza-artificiale/>

<sup>61</sup> Confederazione Svizzera, *Strategia Cina 2021-2024*, [https://www.eda.admin.ch/dam/eda/it/documents/publications/SchweizerischeAussenpolitik/Strategie\\_China\\_210319\\_IT.pdf](https://www.eda.admin.ch/dam/eda/it/documents/publications/SchweizerischeAussenpolitik/Strategie_China_210319_IT.pdf)

La strategia e i principi di regolamentazione IA sono strettamente legati al duplice obiettivo prioritario della Cina di contrastare l'influenza delle Big Tech e diventare leader mondiale dell'IA entro il 2030.

Il Ministero della Scienza e della Tecnologia (MOST) cinese ha inoltre emanato le linee guida per l'IA ("Specifiche etiche per l'intelligenza artificiale di nuova generazione"), delinea sei principi di base per i sistemi di intelligenza artificiale, inclusa la garanzia che siano "controllabili e affidabili".

Gli altri principi consistono nel migliorare il benessere umano, promuovere equità e giustizia, proteggere la privacy e la sicurezza e aumentare il livello di alfabetizzazione etica.

L'approccio cinese è stato certamente influenzato dai valori confuciani e dall'ideologia del socialismo cinese, basata su una concezione dell'essere umano di tipo collettivista e utilitarista, caratterizzato da un'attenzione particolare per la coesione e l'armonia sociale che implica anche un bilanciamento tra diritti civili e controllo morale e di sorveglianza da parte del governo<sup>62</sup>.

Per un'analisi dettagliata della produzione normativa nell'Unione Europea si rimanda al capitolo successivo.

#### **Quarto livello: autoregolamentazione sulla base di principi etici e norme tecniche (ITU, IEEE, ISO/IEC)**

La ITU (*International Telecommunication Union*, ossia l'Unione internazionale delle telecomunicazioni) è una agenzia della Nazioni Unite con competenza per le ICT (*Information and Telecommunication Technologies*, ovvero le tecnologie dell'informazione e della comunicazione). Questa opera nel campo dello sviluppo ed uso dell'intelligenza artificiale per garantire un futuro sostenibile: a tal fine, convoca dialoghi inter governativi e multilaterali, contribuisce allo sviluppo di capacità e standard per l'uso dell'IA<sup>63</sup>.

---

<sup>62</sup> Nanni S., *Cina: le linee guida etiche per l'uso dell'intelligenza artificiale*, 28 ottobre 2021, <https://www.agendadigitale.eu/cultura-digitale/cina-le-linee-guida-etiche-per-luso-dellintelligenza-artificiale/>

<sup>63</sup> ITU, *Artificial Intelligence*, <https://www.itu.int/en/ITU-T/AI/Pages/default.aspx>

Tra le attività ed i documenti prodotti dalla ITU si evidenziano:

- L'*AI for Good Global Summit* annuale, che mira a collegare gli innovatori nel campo dell'IA con i responsabili delle decisioni del settore pubblico e privato per sviluppare strategie e soluzioni di intelligenza artificiale che potrebbero aiutare a raggiungere gli obiettivi di sviluppo sostenibile (SDG)<sup>64</sup>.
- Diverse piattaforme ITU aperte che promuovono vari aspetti dell'intelligenza artificiale e dell'apprendimento automatico, tra cui il Focus Group concernente il machine learning per le future generazioni<sup>65</sup> o il Focus Group relativo alla IA nel settore della salute<sup>66</sup>.

Lo IEEE (*Institute of Electrical and Electronics Engineers*) ha inoltre avviato un programma per affrontare le questioni etiche sollevate dallo sviluppo e dalla diffusione dei sistemi di IA (*Global Initiative on Ethics of Autonomous and Intelligent Systems*<sup>67</sup>), pubblicando nel 2016 una serie di principi direttori per i sistemi IA<sup>68</sup>. In tale quadro, sono stati approvati diversi progetti di standardizzazione approvati che sono attualmente in fase di sviluppo con la IEEE Standards Association.

### **Quinto livello: Normatività dei fatti**

In aggiunta ai quattro livelli di regolazione internazionale precedentemente descritti, si può identificare un ulteriore livello, che si può definire “normatività dei fatti sulla scorta dello sviluppo tecnologico”. Questo è costituito da atti che, pur non essendo compiuti con finalità

---

<sup>64</sup> ITU, *AI for Good Global Summit*, 15 maggio 2018, <https://www.itu.int/en/ITU-T/AI/2018/Pages/default.aspx>

<sup>65</sup> ITU, *Focus Group on Machine Learning for Future Networks including 5G*, <https://www.itu.int/en/ITU-T/focusgroups/ml5g/Pages/default.aspx>

<sup>66</sup> ITU, *Whitepaper for the ITU/WHO Focus Group on Artificial Intelligence for Health*, [https://www.itu.int/en/ITU-T/focusgroups/ai4h/Documents/FG-AI4H\\_Whitepaper.pdf](https://www.itu.int/en/ITU-T/focusgroups/ai4h/Documents/FG-AI4H_Whitepaper.pdf)

<sup>67</sup> *The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems*, <https://standards.ieee.org/industry-connections/ec/autonomous-systems/>

<sup>68</sup> IEEE, *Ethically Aligned Design*, 13 dicembre 2016, [https://standards.ieee.org/wp-content/uploads/import/documents/other/ead\\_v1.pdf](https://standards.ieee.org/wp-content/uploads/import/documents/other/ead_v1.pdf)

normative, hanno una rilevanza ed autorevolezza tale da non poter essere ignorati nell'elaborazione della regolamentazione internazionale.<sup>69</sup>

Molte aziende IA stanno inoltre implementando misure di autoregolamentazione con la creazione di codici di condotta o di carte etiche. Un esempio potrebbe essere la “Partnership on AI (Partenariato sulla IA a beneficio dei cittadini e della società) che annovera, tra gli oltre 100 partner, Amazon, Apple, Google, IBM e Microsoft.<sup>70</sup> L'obiettivo di questo partenariato è quello di apportare benefici alla società e alle persone, formulare le migliori pratiche, far progredire la comprensione pubblica dell'IA e di fungere da piattaforma aperta di discussione.

---

<sup>69</sup> Confederazione Svizzera, Dipartimento Federale degli Affari Esteri, 2022: “*Intelligenza artificiale e regolamentazione internazionale – Rapporto all'attenzione del Consiglio Federale*”, 13 aprile 2022, §5.3.5 - <https://www.news.admin.ch/news/message/attachments/71098.pdf>

<sup>70</sup> Partnership on AI, <https://partnershiponai.org/partners/>

## CAPITOLO II

### Quadro generale ed evoluzione della disciplina della privacy

#### 2.1 Ricognizione della disciplina europea

Il termine *privacy* trae le proprie origini dalla celeberrima monografia giuridica “*The Right of Privacy*”<sup>71</sup> del 1890, anno in cui i giuristi statunitensi Louis Brandeis e Samuel Warren concettualizzarono per la prima volta il “*right to be let alone*”, ossia il diritto ad essere lasciati soli in un’accezione principalmente rivolta alla sfera privata, e dunque intesa come tutela dalle intrusioni altrui. Tale definizione non può ritenersi coincidente con quella della tutela dei dati personali, poiché la seconda è un sottoinsieme della *privacy*, ma riflette un’esigenza del tutto attuale: le innovazioni tecnologiche consentono, come evidenziato nel capitolo precedente, di raccogliere grandi quantità di dati in maniera del tutto automatica, specie considerando i progressivi avanzamenti nell’ottimizzazione degli algoritmi e nel campo del *deep learning*. La sopraccitata pubblicazione nacque anche come tentativo da parte di Warren di tutelare la *privacy* della consorte, lamentandone le violazioni alla riservatezza ed osservando come innovazioni quali la fotografia, in combinazione con le macchine da stampa risalenti al contesto storico della monografia in questione, avrebbero consentito di immortalare momenti e dettagli della vita privata altrui e diffonderli rapidamente. Tutto ciò si è accentuato esponenzialmente nell’epoca moderna, sollevando numerosi interrogativi per quanto concerne il quadro giuridico che deve regolare tale campo.

Nell’ottica comunitaria, prima di giungere all’odierna regolamentazione, la questione sinora analizzata non era disciplinata da atti specifici. Rileva anzitutto l’art. 8 della Convenzione Europea sui diritti dell’uomo, firmata nel 1950 dal Consiglio d’Europa e istitutiva della Corte europea dei diritti dell’uomo. La norma citata concerne il “*Rispetto della vita privata e familiare*”, di cui si riporta il testo.

---

<sup>71</sup> Warren S. e Brandeis L., *The Right to Privacy*, Harvard Law Review 193, 1890.



## **Convenzione europea dei diritti dell'uomo - Articolo 8: Diritto al rispetto della vita privata e familiare**

1. *Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.*
2. *Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.*<sup>72</sup>

La giurisprudenza della Corte europea ha definito il campo di applicazione dell'articolo riportato in maniera ampia, talvolta determinandone l'applicabilità anche in base ad un criterio di gravità (ad esempio, un attacco alla reputazione che raggiunge un certo livello di "serietà")<sup>73</sup>, ed è specificamente finalizzato alla tutela dalle ingerenze arbitrarie nella vita privata e familiare, nel domicilio e nella corrispondenza da parte di un'autorità pubblica<sup>74</sup>. La CEDU, dunque, circoscrive il potere degli stati di incidere sulla *privacy* a ipotesi in cui è necessario tutelare i valori cardine della società democratica, nonché i diritti umani. Rileva in particolare anche la Carta dei Diritti fondamentali dell'Unione Europea, elaborata dalla Convenzione europea e ratificata il 7 dicembre 2000 a Nizza dal Parlamento Europeo, il Consiglio dell'Unione europea e la Commissione europea. Nota anche come la Carta di Nizza, essa, per la prima volta nella storia dell'Unione europea, ha elaborato il catalogo completo dei diritti civili, politici, economici e sociali dei cittadini e delle persone residenti nell'Unione europea, dividendoli in sei capi: dignità, libertà, uguaglianza, solidarietà,

---

<sup>72</sup> Consiglio d'Europa, *Convenzione Europea dei diritti dell'uomo*, 1950, art. 8, [https://www.europarl.europa.eu/charter/pdf/text\\_it.pdf](https://www.europarl.europa.eu/charter/pdf/text_it.pdf)

<sup>73</sup> Corte europea dei diritti dell'uomo, *Denisov c. Ucraina*, , 25 settembre 2018, §§ 111-112, [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-186216%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-186216%22]})

<sup>74</sup> Corte europea dei diritti dell'uomo, *Guida all'articolo 8 - Diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza*, aggiornata al 31 agosto 2019, [https://www.echr.coe.int/documents/guide\\_art\\_8\\_ita.pdf](https://www.echr.coe.int/documents/guide_art_8_ita.pdf)

cittadinanza e giustizia. Rilevano per quanto concerne il quadro normativo della *privacy* in una prospettiva comunitaria gli artt. 7 e 8 del capo sulla libertà.

### **Carta di Nizza - Articolo 7: Rispetto della vita privata e della vita familiare**

*Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni.*

### **Carta di Nizza - Articolo 8: Protezione dei dati di carattere personale**

- 1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.*
- 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.*
- 3. Il rispetto di tali regole è soggetto al controllo di un' autorità indipendente.<sup>75</sup>*

L'articolo 8 della Carta di Nizza rivolge maggiore attenzione al trattamento dei dati personali, ed è fondato su diverse norme pregresse inerenti alla materia, tra cui l'art. 286 del trattato che istituisce la comunità europea, che sanciva l'applicazione alle istituzioni ed organismi con esso istituiti degli atti concernenti la protezione delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione degli stessi.<sup>76</sup>

<sup>75</sup> Carta dei diritti fondamentali dell'Unione europea, [https://www.europarl.europa.eu/charter/pdf/text\\_it.pdf](https://www.europarl.europa.eu/charter/pdf/text_it.pdf)

<sup>76</sup> Trattato che istituisce la Comunità europea (versione consolidata Maastricht), Parte sesta: Disposizioni generali e finali, gazzetta ufficiale n. C 340 del 10 novembre 1997, pag. 0294 - versione consolidata, art. 286, <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A11997E286>

L'articolo 286 questione è stato oggi sostituito dal dispositivo dell'art. 16 del Trattato sul funzionamento dell'Unione europea (TFUE), nonché dall'art. 39 del Trattato sull'Unione europea (TUE).<sup>77</sup>

### **Trattato sul funzionamento dell'Unione europea – Articolo 16**

- 1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.*
- 2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti.*

*Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea.*<sup>78</sup>

### **Trattato sull'Unione europea – Articolo 39**

*Conformemente all'articolo 16 del trattato sul funzionamento dell'Unione europea e in deroga al paragrafo 2 di detto articolo, il Consiglio adotta una decisione che stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del presente capo, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti.*<sup>79</sup>

<sup>77</sup> FRA – European Union Agency for fundamental rights, *Article 8 – Protection of personal data*, <https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data#explanations>

<sup>78</sup> Trattato sul funzionamento dell'Unione europea (versione consolidata), art. 16, <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:12012E/TXT>

<sup>79</sup> Trattato sull'Unione europea (versione consolidata), art. 39, [https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0017.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0017.02/DOC_1&format=PDF)

Gli articoli citati offrono, dunque, un quadro normativo della tutela dei dati di carattere personale, sancendo il diritto di ogni persona (pertanto non solo cittadini) alla protezione degli stessi, di cui si discuterà più approfonditamente nel contesto del GDPR.

Oltre alle norme di portata generale sinora riportate, tre direttive della Comunità europea ampliarono ulteriormente il quadro normativo del trattamento dei dati personali. La direttiva 1995/46/CE concerne la “*tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*”<sup>80</sup>. Rilevano anche le direttive 1997/66/CE sul “*trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni*”<sup>81</sup>, e 2002/58/CE sul “*trattamento dei dati personali e la tutela della vita privata nel settore delle comunicazioni elettroniche*”.<sup>82</sup>

La direttiva 1995/46/CE, avente lo scopo di armonizzare le legislazioni nazionali per favorire la circolazione dei dati nella Comunità Economica Europea<sup>83</sup>, offre spunti di particolare rilevanza per la presente trattazione, poiché introduce disposizioni precise sulla materia. Ai sensi dell’art. 1 del Capo I,

#### **Direttiva 1995/46/CE: Art. 1**

*Gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali.*<sup>84</sup>

Il legislatore europeo, dunque, mosse i primi passi verso l’apertura del traffico dei dati personali. Gli Stati membri, a loro volta, dovevano operare un compromesso con riguardo al trattamento dei dati personali, tutelando l’esigenza di tutela dei diritti e delle libertà

<sup>80</sup> Direttiva 1995/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A31995L0046>

<sup>81</sup> Direttiva 1997/66/CE del Parlamento europeo e del Consiglio del 15 dicembre 1997, <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A31997L0066>

<sup>82</sup> Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, <https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX%3A32002L0058>

<sup>83</sup> Pizzetti F., *Intelligenza Artificiale, protezione dei dati personali e regolazione*, Giappichelli, 2018, p. 8

<sup>84</sup> Direttiva 1995/46/CE, *supra*, art. 1, Capo I.

fondamentali delle persone fisiche, senza compromettere la libera circolazione di tali dati tra i Paesi medesimi.

Come nel caso dell'intelligenza artificiale, non vi è una definizione universale del termine; uno studio condotto tra il 2001 e il 2002 ne ha definito il relativo modello di crescita come *tridimensionale* o *modello delle "3V"*, facendo riferimento al volume, ossia la quantità di dati provenienti da diverse fonti; le diverse tipologie di dati, ergo la varietà; e la velocità con cui questi sono generati.<sup>85</sup> Segue la lettera dell'art. 2 della Direttiva 95/46/CE.

#### **Direttiva 1995/46/CE: Art. 2**

*Ai fini della presente direttiva si intende per:*

- a) «**dati personali**»: qualsiasi informazione concernente una persona fisica identificata o identificabile («persona interessata»); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale;*
- b) «**trattamento di dati personali**» («trattamento»): qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione;*
- c) «**archivio di dati personali**» («archivio»): qualsiasi insieme strutturato di dati personali accessibili, secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;*

---

<sup>85</sup> Agenda Digitale, Amato S., *Big data: cosa sono, tipologie, esempi e sfide dell'economia del dato*, 18 maggio 2020, <https://www.agendadigitale.eu/cittadinanza-digitale/big-data-cosa-sono-tipologie-esempi-e-sfide-delleconomia-del-dato/>

- d) **«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 al sua designazione possono essere fissati dal diritto nazionale o comunitario;
- 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;
- f) **«terzi»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che non sia la persona interessata, il responsabile del trattamento, l'incaricato del trattamento e le persone autorizzate all'elaborazione dei dati sotto la loro autorità diretta;
- g) **«destinatario»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che riceve comunicazione di dati, che si tratti o meno di un terzo. Tuttavia, le autorità che possono ricevere comunicazione di dati nell'ambito di una missione d'inchiesta specifica non sono considerate destinatari;
- h) **«consenso della persona interessata»**: qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento.<sup>86</sup>

La norma in esame definiva alcuni dei concetti più ricorrenti nell'ambito della tutela dei dati personali, intesi come informazioni volte a identificare persone e trattate anche con l'ausilio di *processi automatizzati*, per l'archiviazione, l'utilizzazione e la diffusione delle stesse con il consenso informato della persona interessata.

Non figuravano nella normativa in esame riferimenti specifici all'intelligenza artificiale come delineata nel Capitolo I, in quanto i sistemi per l'analisi dei *big data* non avevano raggiunto il livello di sviluppo odierno. Il termine in questione fa riferimento alle operazioni di gestione e

---

<sup>86</sup> Direttiva 95/46/CE, art. 2.

analisi di grandi quantità di dati, raccolti da numerose fonti quali internet, i social media, i cellulari, le applicazioni multimediali, gli archivi commerciali, le statistiche, gli strumenti di geolocalizzazione ed i pagamenti online.

L'art. 3 della direttiva specifica che le disposizioni della stessa si applicavano, con alcune eccezioni, al *trattamento di dati personali interamente o parzialmente automatizzato*<sup>87</sup>; inoltre, l'art. 5 stabiliva che gli Stati membri devono precisare le condizioni alle quali i trattamenti dei dati personali sono leciti.<sup>88</sup> La direttiva ha anche costituito il Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, che studia i problemi legati alla tutela dei dati individuali nell'ambiente di lavoro e la cui normativa sarà successivamente richiamata nel GDPR.

L'art. 29<sup>89</sup> dispone che il gruppo ha carattere "*consultivo e indipendente*", e i relativi compiti sono disciplinati dal successivo art. 30<sup>90</sup>. In particolare, questo deve esaminare le questioni inerenti all'applicazione delle norme nazionali e di attuazione della Direttiva, formulando pareri sul "*livello di tutela nella Comunità e nei paesi terzi*".

Il Gruppo ha fornito anche una definizione del sopraccitato concetto di *big data*, definendolo come la crescita esponenziale sia nella disponibilità, sia nel trattamento automatizzato dell'informazione, riferendosi alle grandi quantità di dati in forma digitale in mano ad aziende, governi ed altre grandi organizzazioni, i quali sono poi analizzati estensivamente utilizzando algoritmi computerizzati. Il Parere in questione specifica anche che i *big data* sono utilizzabili per identificare tendenze e correlazioni, ma possono anche essere elaborati in modo tale da incidere direttamente sugli individui.<sup>91</sup>

---

<sup>87</sup> Direttiva 95/46/CE, art. 3.

<sup>88</sup> Direttiva 95/46/CE, art. 5.

<sup>89</sup> Direttiva 95/46/CE, art. 29.

<sup>90</sup> Direttiva 95/46/CE, art. 30.

<sup>91</sup> Parere 3/2013 del *Data Protection Working Party*, 2 Aprile 2013, p. 35, [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf)

## 2.2 Ricognizione della disciplina nazionale

La direttiva 1995/46/CE sinora esaminata ha inciso sul quadro storico della disciplina del trattamento dei dati personali in Italia, poiché determinò l'adozione della l. n. 675 del 31 dicembre 1996, entrata in vigore nel maggio 1997, inerente alla “*tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*”<sup>92</sup>. successivamente abrogata dal d.lgs. 30 giugno 2003, n. 196 (*Codice in materia di protezione dei dati personali*)<sup>93</sup>.

L'art. 1 del Capo I sui principi generali concerne le finalità e definizioni della legge in questione, stabilendo quanto segue nel comma I:

### **L. n. 675/1996 - Art. 1, comma I: finalità e definizioni**

*La presente legge garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale; garantisce altresì i diritti delle persone giuridiche e di ogni altro ente o associazione.*<sup>94</sup>

La legge opera un richiamo all'art. 1 della Convenzione del Consiglio d'Europa n. 108, adottata a Strasburgo il 28 gennaio 1981, il cui oggetto è ricalcato dalla Direttiva 1995/46/CE. Tale norma concerne il *rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano (protezione dei dati)*<sup>95</sup>.

<sup>92</sup> L. n. 675 del 31 dicembre 1996 - *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*, <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/28335>

<sup>93</sup> Decreto legislativo 30 giugno 2003, n. 196 - *Codice in materia di protezione dei dati personali*, <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30:196>

<sup>94</sup> L. n. 675 del 31 dicembre 1996, *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*, *supra*, art. 1.

<sup>95</sup> Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, Strasburgo, 28 gennaio 1981, Traduzione ufficiale della Cancelleria federale della Svizzera, <https://rm.coe.int/1680078c45>



Essa impone di garantire ad ogni persona fisica sul territorio delle Parti (non necessariamente membri del Consiglio d'Europa) il rispetto del diritto alla vita privata, con particolare riguardo all'elaborazione automatica dei dati a carattere personale che la riguardano. È implicitamente richiamato anche il già esaminato art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo.<sup>96</sup>

La norma, facendo espresso riferimento alla tutela della *dignità della persona*, nonché alla *riservatezza* e all'*identità personale*, introduce un diritto sui propri dati personali, la cui tutela prescinde dall'avvenuta comunicazione e diffusione o dalla eventuale lesione del valore sociale dell'individuo. Essa concerne un elenco non tassativo di attività di raccolta, elaborazione, comunicazione, diffusione ed utilizzo dei dati in questione, proteggendo preventivamente le persone fisiche da un potere tanto incisivo<sup>97</sup>; esigenza, questa, avvertita già dal legislatore del 1996 e del tutto attuale, in ragione del fatto che la raccolta di dati è divenuta sempre più intrusiva a mezzo dei moderni strumenti elettronici.

L'articolo 2 della Convenzione di Strasburgo del 1981 definisce i *dati a carattere generale* come *ogni informazione concernente una persona fisica identificata o identificabile*.<sup>98</sup> La nozione di *dati personali* nella legge 675/96 coincide sostanzialmente con quella fornita dalla Convenzione, ma si distingue in quanto si applica anche alle persone giuridiche, gli enti e le associazioni; non si limita, dunque, alle sole persone fisiche, fornendo anche criteri per considerare identificabile la persona. Con riguardo all'automatizzazione del trattamento dei dati, la Convenzione disciplina solo le banche dati elettroniche o automatizzate.

---

<sup>96</sup> Giannantonio E., Losano M. G., Zeno-Zencovich V., *La tutela dei dati personali – Commentario alla l. 675/1996*, CEDAM – Padova, 1997, p. 2

<sup>97</sup> Giannantonio E., Losano M. G., Zeno-Zencovich V., *La tutela dei dati personali – Commentario alla l. 675/1996*, CEDAM – Padova, 1997, p. 5

<sup>98</sup> Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, Strasburgo, Traduzione ufficiale della Cancelleria federale della Svizzera, 28 gennaio 1981, <https://rm.coe.int/1680078c45>

In particolare, nel contesto degli *schede automatizzati*, fa riferimento ad *insiemi di informazioni oggetto di elaborazione automatica* comprendenti *operazioni svolte in tutto o in parte con mezzi automatizzati*; viceversa, la legge n. 675/1996 estende la protezione dei dati anche al trattamento dei dati nelle ipotesi in cui non sussista l'ausilio dei mezzi in questione.<sup>99</sup>

Segue la lettera del comma II dell'art. 1<sup>100</sup>, che fornisce un elenco di nozioni non dissimile da quello dell'art. 2 della direttiva 95/46/CE.

### **L. n. 675/1996 - Articolo 1, comma II: finalità e definizioni**

2. Ai fini della presente legge si intende:

a) per "**banca di dati**", qualsiasi complesso di dati personali, ripartito in una o più unità dislocate in uno o più siti, organizzato secondo una pluralità di criteri determinati tali da facilitarne il trattamento.

b) per "**trattamento**", qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati.

c) per "**dato personale**", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

<sup>99</sup> Giannantonio E., Losano M. G., Zeno-Zencovich V., *La tutela dei dati personali – Commentario alla l. 675/1996*, CEDAM – Padova, 1997, p. 16

<sup>100</sup> L. n. 675 del 31 dicembre 1996 - *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*, art. 1, comma II, <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/28335>

d) 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) 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;

f) per "**interessato**", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

g) per "**comunicazione**", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

h) per "**diffusione**", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

i) per "**dato anonimo**", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

l) per "**blocco**", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

m) per "**Garante**", l'autorità istituita ai sensi dell'articolo 30.

Il *trattamento*, dunque, era definito come qualsiasi operazione avente ad oggetto dati suscettibili di essere associati ad una persona fisica o giuridica, indipendentemente dal mezzo utilizzato.<sup>101</sup> Inoltre, la giurisprudenza tentò a suo tempo di definire il termine *banca dati* ("o *archivio o indirizzario computerizzato*") come "un *quid* dotato di autonomo ed originale contenuto economico".<sup>102</sup>

<sup>101</sup> Giannantonio E., Losano M. G., Zeno-Zencovich V., *La tutela dei dati personali – Commentario alla l. 675/1996*, CEDAM – Padova, 1997, p. 19

<sup>102</sup> Tribunale di Genova, 19 giugno 1993, *Dir. Inf.*, 1993, 1117.

Sia la legge 675/96, sia la Direttiva 1995/46/CE definiscono una figura responsabile del trattamento dei dati personali (ex art. 2 della Direttiva, *incaricato del trattamento*), nonché un titolare delle decisioni; nozioni, queste, riscontrabili nell'odierno GDPR.

Con riguardo al trattamento automatizzato, la legge 675/96 imponeva dei limiti concernenti la *valutazione del comportamento umano*:

**L. n. 675/1996 - Art. 17: Limiti all'utilizzabilità di dati personali**

*1. Nessun atto o provvedimento giudiziario o amministrativo che implichi una valutazione del comportamento umano può essere fondato unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato.*

*2. L'interessato può opporsi ad ogni altro tipo di decisione adottata sulla base del trattamento di cui al comma 1 del presente articolo, ai sensi dell'articolo 13, comma 1, lettera d), salvo che la decisione sia stata adottata in occasione della conclusione o dell'esecuzione di un contratto, in accoglimento di una proposta dell'interessato o sulla base di adeguate garanzie individuate dalla legge.*

La norma concerne la valutazione del comportamento umano nelle ipotesi della presa di decisioni sulla base di profili automatizzati. Consentendo la tecnologia informatica di costruire automaticamente profili individuali e collettivi, nonché in taluni casi adottare decisioni in autonomia sul conto dei soggetti interessati utilizzando i dati in uno o più archivi, che vengono elaborati a tali scopi. Ciò comporta un rischio per l'individuo, potendo questi essere potenzialmente leso da un'elaborazione basata su dati decontestualizzati, specialmente in contesti quali quello dei rapporti di lavoro, potendo già essere disposti con gli algoritmi dell'epoca, ad esempio, profili psicologici ideali relativi ad un determinato impiego.<sup>103</sup>

---

<sup>103</sup> Giannantonio E., Losano M. G., Zeno-Zencovich V., *La tutela dei dati personali – Commentario alla l. 675/1996, CEDAM – Padova*, 1997, pp. 165-167

L'art. 30 della legge 675/96 è di fondamentale importanza, poiché istituisce la figura del Garante per la protezione dei dati personali.

**L. n. 675/1996 - Art. 30, commi I e II: Istituzione del Garante**

*1. è istituito il Garante per la protezione dei dati personali.*

*2. Il Garante opera in piena autonomia e con indipendenza di giudizio e di valutazione.*

Trattasi, dunque, di un'autorità amministrativa autonoma nell'esercizio delle proprie funzioni di vigilanza nell'ambito della protezione dei dati personali. I relativi membri *sono scelti tra persone che assicurino indipendenza e che siano esperti di riconosciuta competenza delle materie del diritto o dell'informatica, garantendo la presenza di entrambe le qualificazioni.*<sup>104</sup> Oggi, ai sensi dell'art. 51 del GDPR, il Garante è l'autorità di controllo designata ai fini dell'attuazione di tale regolamento.<sup>105</sup>

La Convenzione del Consiglio d'Europa sopraccitata non prevedeva esplicitamente l'istituzione di autorità quali il Garante; era tuttavia già possibile osservare degli sviluppi in tal senso a partire dalla Convenzione di Dublino del 15 giugno 1990 concernente il diritto d'asilo, successivamente ratificata dall'Italia con legge n. 523/1992, che come l'Accordo di Schengen e la successiva Convenzione di applicazione, ratificati con legge n. 388 del 1993, prevedevano la realizzazione del "Sistema Informativo Schengen", volto a permettere la circolazione di dati relativi alle persone con finalità attinenti sicurezza e ordine pubblico.

La norma, inoltre, ottempera ad un obbligo imposto dall'ordinamento comunitario nella Direttiva 95/46/CE, che riteneva necessaria l'istituzione negli Stati membri di autorità efficaci e pienamente indipendenti nell'esercizio delle loro funzioni, poste al centro del sistema di notificazione dei trattamenti e dei controlli preliminari o successivi, nonché

<sup>104</sup> L. n. 675 del 31 dicembre 1996 - *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*, <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/28335>

<sup>105</sup> GPDP, *Il garante*, <https://www.garanteprivacy.it/home/autorita>

provviste di poteri autoritativi di natura ispettiva e inibitoria, al fine di tutelare le persone nel contesto del trattamento dei dati che le riguardano.<sup>106</sup>

L'art. 31 della legge in esame descriveva estensivamente i compiti del Garante, che, in qualità di centro istituzionale di osservazione sul sistema della tutela del diritto alla riservatezza riguardo ai contenuti delle banche dati, acquisisce informazioni svolgendo funzioni di ricognizione dei soggetti operanti nel settore, nonché per quanto concerne la corrispondenza tra soggetti presenti e risultanti dal sistema di pubblicità relativo al registro.<sup>107</sup>

In particolare, svolge funzioni di vigilanza sull'effettuazione dei trattamenti nel rispetto delle norme di legge, segnalando ai titolari o responsabili le modificazioni necessarie al fine di renderne l'operato conforme alle disposizioni vigenti. Il *registro generale dei trattamenti sulla base delle notificazioni ricevute* è menzionato nella lettera a) dell'articolo sopraccitato, che ne prevede l'istituzione da parte del Garante.

## 2.3 Cenni introduttivi al GDPR

Il *regolamento generale sulla protezione dei dati*, noto in inglese come *General Data Protection Regulation*, è stato adottato il 27 aprile 2016 e promulgato il 25 maggio 2018, e concerne la *protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*<sup>108</sup>. La direttiva 1995/46/CE sopraccitata fu definitivamente abrogata, comportando conseguentemente la disapplicazione delle norme nazionali preesistenti ove in contrasto con il GDPR.

---

<sup>106</sup> Giannantonio E., Losano M. G., Zeno-Zencovich V., *La tutela dei dati personali – Commentario alla l. 675/1996, CEDAM – Padova*, 1997, p. 293

<sup>107</sup> Giannantonio E., Losano M. G., Zeno-Zencovich V., *La tutela dei dati personali – Commentario alla l. 675/1996, CEDAM – Padova*, 1997, p. 318

<sup>108</sup> Regolamento (UE) 2016/679 del parlamento europeo e del consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32016R0679>

Il riconoscimento del diritto alla protezione dei dati personali come diritto fondamentale dei cittadini europei deriva dall'art. 8 della Carta dei diritti fondamentali, che fa specifico riferimento a "persone", nonché dall'art. 16 del TFUE, e costituisce il fondamento della scelta del legislatore sopranazionale nel settore<sup>109</sup>. Il Trattato di Lisbona<sup>110</sup>, firmato il 13 dicembre 2007 ed entrato in vigore il 1° dicembre 2009, ha infatti attribuito alla Carta di Nizza il valore giuridico dei trattati, comportando l'obbligo del parlamento europeo di conformarsi al quadro normativo così delineato.

Anche in questo caso il Regolamento non fa specifico riferimento all'intelligenza artificiale come successivamente definita nella proposta di regolamento in materia di AI; nondimeno, esso amplia la protezione delle persone fisiche nell'ambito del trattamento manuale e automatizzato dei dati personali, "*se i dati personali sono contenuti o destinati a essere contenuti in un archivio*"<sup>111</sup>.

Con riguardo all'effetto abrogativo del GDPR, l'art. 94 del Capo XI concernente le disposizioni finali sancisce quanto segue.

#### **Regolamento 2016/679 - Articolo 94: Abrogazione della direttiva 95/46/CE**

1. *La direttiva 95/46/CE è abrogata a decorrere da 25 maggio 2018.*
2. *I riferimenti alla direttiva abrogata si intendono fatti al presente regolamento. I riferimenti al gruppo per la tutela delle persone con riguardo al trattamento dei dati personali istituito dall'articolo 29 della direttiva 95/46/CE si intendono fatti al comitato europeo per la protezione dei dati istituito dal presente regolamento.*

<sup>109</sup> Pizzetti F., *Intelligenza Artificiale, protezione dei dati personali e regolazione*, G. Giappichelli Editore, ed. 2018, p. 8

<sup>110</sup> Trattato di Lisbona che modifica il trattato sull'Unione Europea e il trattato che istituisce la Comunità europea, <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A12007L%2FTXT>

<sup>111</sup> Regolamento 2016/679, Considerando 15.

La disposizione ha comportato il riordino del sistema delle fonti del diritto dell'Unione europea in materia di protezione dei dati personali, evitando sovrapposizioni tra diverse fonti del diritto. Occorre analizzare in tal senso alcune pronunce della Corte di Giustizia, volte in parte a rendere più semplice l'interpretazione del diritto positivo vigente in seguito all'adozione del GDPR. La sentenza resa nel caso *Schrems*<sup>112</sup> è di fondamentale rilevanza nel contesto del rapporto tra il GDPR, il relativo art. 94 e l'effetto abrogativo nei confronti della Direttiva 95/46/CE. La pronuncia concerne una controversia tra il Commissario per la protezione dei dati irlandese, Facebook Ireland Ltd. ed il sig. Maximillian Schrems, che sporse denuncia presso quest'ultimo relativamente al trasferimento dei suoi dati personali da parte di Facebook Ireland Ltd. a Facebook Inc. negli Stati Uniti. I governi tedesco e del Regno Unito sostenevano che la pronuncia pregiudiziale richiesta era irricevibile, poiché *“le disposizioni della direttiva 95/46/CE sulle quali si fondano le questioni pregiudiziali sono state abrogate dal (GDPR)”*. La Corte ha ribadito il proprio orientamento secondo il quale essa *“ha il compito di interpretare tutte le disposizioni del diritto dell'Unione che possano essere necessarie ai giudici nazionali al fine di dirimere le controversie per le quali sono stati aditi, anche qualora tali disposizioni non siano espressamente indicate nelle questioni ad essa sottoposte da detti giuridici”*: in tal senso, le previsioni indicate nelle questioni pregiudiziali sono state ritenute riprese sostanzialmente da specifici articoli del Regolamento.<sup>113</sup>

---

<sup>112</sup> CGUE, C-311/18, Data Protection Commissioner c. Facebook Ireland Ltd., Maximillian Schrems, 16 luglio 2020.

<sup>113</sup> Riccio G. M., Scorza G., Belisario E., *GDPR e Normativa Privacy – Commentario*, Wolters Kluwer, 2022, p. 823.



## CAPITOLO III

### Intelligenza artificiale e trattamento automatizzato dei dati personali

#### 3.1 Il regolamento generale sulla protezione dei dati

A partire dall'entrata in vigore del GDPR nel mese di maggio 2018, gli stati dell'Unione europea e numerosi settori dell'economia si sono adattati al quadro normativo delineato dal Regolamento. La presente trattazione analizzerà specificamente i punti di incontro fra la normativa in esame e il trattamento automatico dei dati reso possibile dagli algoritmi di intelligenza artificiale, focalizzandosi sui problemi giuridici e le relative sfide.

Come precedentemente menzionato, il GDPR concerne la *protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*; in quanto tale, gli Stati membri devono assicurare il rispetto dei principi in esso contenuti. Ciò scaturisce dalla lettera degli artt. 16 TFUE e 8 della Carta, i quali stabiliscono che il Parlamento e il Consiglio hanno l'obbligo di dettare la normativa volta alla protezione dei dati personali a tutela delle persone fisiche.

Poiché tale tutela è riconosciuta come diritto fondamentale, le norme europee non saranno rivolte alle sole istituzioni ed organi dell'Unione, ma si traducono in principi vincolanti per gli Stati membri. La disciplina contenuta nel GDPR può essere integrata dalla legislazione nazionale, ma gli Stati membri devono attenersi ai vincoli delineati nel Regolamento, o viceversa escluderne parzialmente l'applicazione.<sup>114</sup>

---

<sup>114</sup> Pizzetti F., *Intelligenza Artificiale, protezione dei dati personali e regolazione*, Giappichelli, 2018, p.10.

Ai sensi dell'art. 23 del GDPR, *“il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti”* elencati in specifiche disposizioni, *“qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare”* numerosi diritti ed ambiti del trattamento dei dati.

Ai fini della presente trattazione rilevano in particolare le *finalità del trattamento o le categorie di trattamento, le categorie di dati personali, le garanzie per prevenire abusi o l'accesso o il trasferimento illeciti, nonché i periodi di conservazione e le garanzie applicabili tenuto conto della natura, dell'ambito di applicazione e delle finalità del trattamento o delle categorie di trattamento.*<sup>115</sup>

Occorre sottolineare come il diritto sin qui esaminato debba essere valutato in base al *principio di proporzionalità* delineato nel Considerando 4, *“alla luce della sua funzione sociale e va temperato con altri diritti fondamentali”*<sup>116</sup>; ciò è in linea con quanto disposto dall'art. 52 della Carta, che cita il principio di necessità e proporzionalità in riferimento ai possibili limiti dei diritti fondamentali.<sup>117</sup>

I diritti sinora citati sono enunciati sinteticamente nell'art. 1 del Regolamento.

---

<sup>115</sup> Regolamento 2016/679, art. 23.

<sup>116</sup> Regolamento 2016/679, Considerando 4.

<sup>117</sup> Riccio G. M., Scorza G., Belisario E., *GDPR e Normativa Privacy – Commentario*, Wolters Kluwer, 2022, p. 293.

## **Regolamento 2016/679 – Articolo 1: Oggetto e finalità**

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

Il legislatore europeo pone particolare enfasi anche sulla libertà di circolazione dei dati, in accordo con l'oggetto della Direttiva 95/46/CE, concetto di grande di rilevanza se rapportato con l'automatizzazione del trattamento dei dati nel contesto odierno, ove anche agenti economici di piccole dimensioni si trovano ormai frequentemente di fronte alla necessità di gestire e muovere grandi quantità di dati sensibili dei propri clienti.

Rileva in tal senso anche il Considerando 2, che menziona fra le finalità del Regolamento la *realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica volta al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche*<sup>118</sup>.

Quanto all'ambito di applicazione materiale del Regolamento, l'art. 2 stabilisce nel 1° comma che esso *“si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi”*.

---

<sup>118</sup> Regolamento 2016/679, Considerando 2.

Rileva in tal senso anche il Considerando 15:

**Regolamento 2016/679 – Considerando 15:**

*Al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate. La protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati a essere contenuti in un archivio. Non dovrebbero rientrare nell'ambito di applicazione del presente regolamento i fascicoli o le serie di fascicoli non strutturati secondo criteri specifici, così come le rispettive copertine.*

Il principio enunciato nel Considerando 15, concernente la neutralità tecnologica, è stato dunque recepito dall'art. 2 del GDPR, con la sola eccezione dei dati destinati a figurare negli archivi, come definiti al n. 6 dell'art 4, ossia “*qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico*”.<sup>119</sup>

### 3.2 Il trattamento automatizzato

Ai fini della presente trattazione, la profilazione e i processi decisionali svolti mediante algoritmi, entrambi menzionati nell'art. 22 GDPR, sono di fondamentale rilevanza. Prima di correre anzitutto definire il quadro normativo relativo al trattamento automatizzato dei dati personali.

L'articolo 4 del GDPR fornisce un elenco delle nozioni utilizzate dal Regolamento, che anche in questo caso non fa riferimento esplicito all'intelligenza artificiale. Il “dato personale” oggetto del trattamento è oggi definito come segue:

---

<sup>119</sup> Riccio G. M., Scorza G., Belisario E., *GDPR e Normativa Privacy – Commentario*, Wolters Kluwer, 2022, p. 12.

## **Regolamento 2016/679 – Articolo 4: Definizioni**

*Ai fini del presente regolamento s'intende per:*

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

La nozione riportata risale alla Convenzione 108/1981, recepita nell'articolo 4 della Direttiva 95/46/CE. Il dato è costituito da quattro elementi:

- *Informazione*: una rappresentazione in qualsiasi formato di cose, fatti o persone suscettibile di circolazione;
- *Persona fisica*: l'«interessato», inteso come il soggetto cui l'informazione è collegata;
- *Collegamento*: l'operazione il trattamento automatizzato opererà secondo un criterio logico;
- *Identificazione / identificabilità*: concetto riferito alla persona fisica, a sua volta scomponibile in più elementi:
  - *Identificativo*: trattasi dell'informazione o elemento informativo presente nel dato personale, non necessariamente coincidente col nome anagrafico (che, anzi, può risultare irrilevante).
  - *Identificazione*: l'individuazione e riconoscimento della persona resa possibile dall'identificativo all'interno di uno specifico contesto.
  - *Identificabilità*: la possibilità concreta di operare il processo di identificazione sopra definito a mezzo degli strumenti a disposizione del titolare del trattamento o del terzo.<sup>120</sup>

---

<sup>120</sup> Bolognini L., Pelino E., Bistolfi C., *Il regolamento privacy europeo – Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè, 2016, pp. 44-50.

L'art. 4 definisce anche i dati genetici, biometrici e relativi alla salute<sup>121</sup> che possono essere raccolti con le operazioni di trattamento automatizzato.

La nozione di trattamento fornita dal GDPR non menziona esplicitamente l'intelligenza artificiale, ma i relativi algoritmi rientrano nella definizione fornita dall'art. 4, che definisce come segue i processi automatizzati concernenti i dati personali come precedentemente delineati:

#### **Regolamento 2016/679 – Articolo 4: Definizioni**

2) *«trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali [...];*

3) *«limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;<sup>122</sup>*

Le operazioni ivi menzionate formano un elenco da ritenersi esemplificativo, in ragione del fatto che, come osservato nell'opinione 1/2015 del Gruppo di Lavoro per la Protezione dei dati "Articolo 29", l'uso di droni per la raccolta di dati, anche senza registrazione o conservazione, "costituisce nondimeno un'operazione di trattamento che comporta l'applicazione della normativa in materia di protezione dei dati personali". L'applicazione della relativa normativa scongiura in parte i rischi di *mass surveillance* menzionati nel corso della presente trattazione, in ragione della sempre maggiore intrusività ed efficienza delle nuove tecnologie in ambito AI.

<sup>121</sup> Regolamento 2016/679, art. 4, comma I, nn. 13, 14, 15.

<sup>122</sup> Regolamento 2016/679, art. 4, comma I, nn. 2 e 3.

L'articolo 4 menziona i seguenti esempi di operazioni di trattamento automatizzato. La realizzazione di anche una sola di esse renderà applicabile la normativa del Regolamento<sup>123</sup>:

- Raccolta;
- Registrazione;
- Organizzazione;
- Strutturazione;
- Conservazione;
- Adattamento o modifica;
- Estrazione;
- Consultazione;
- Uso;
- Comunicazione mediante:
  - Trasmissione;
  - Diffusione;
  - Altre forme di messa a disposizione;
- Raffronto o interconnessione;
- Limitazione;
- Cancellazione o distruzione.

Le operazioni di trattamento, dunque, sono eterogenee, e la normativa sinora riportata non specifica che esse debbano essere necessariamente portate a compimento con processi automatizzati. In particolare, il termine *trattamento* è riferito all'attività del trattare dati, ed ha una connotazione sostanzialmente tecnica.<sup>124</sup> Non sussistono particolari problemi per quanto concerne la sussunzione degli algoritmi IA nel quadro normativo definito dall'art. 4 del GDPR.

---

<sup>123</sup> Riccio G. M., Scorza G., Belisario E., *GDPR e Normativa Privacy – Commentario*, Wolters Kluwer, 2022, p.55-56.

<sup>124</sup> Bolognini L., Pelino E., Bistolfi C., *Il regolamento privacy europeo – Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè, 2016, pp. 88.

La “*limitazione di trattamento*” successivamente menzionata consiste nella possibilità per l’interessato di ottenere richiedere al titolare del trattamento con esplicita richiesta la sola conservazione dei dati personali, impedendone temporaneamente l’utilizzo o l’accesso.

Il Regolamento sancisce nell’art. 5, con riguardo al trattamento automatizzato dei dati, i principi di *liceità, correttezza e trasparenza*. La norma rientra nel Capo II, che descrive le condizioni della legittimità del trattamento.

### **Regolamento 2016/679 – Art. 5: Principi applicabili al trattamento di dati personali**

1. *I dati personali sono:*

a) *trattati in modo lecito, corretto e trasparente nei confronti dell’interessato («liceità, correttezza e trasparenza»);*

Il principio di *liceità*, dall’inglese *lawfulness*, è inquadrabile come un più generale parametro di valutazione della conformità del diritto al trattamento. Il successivo art. 6 del Regolamento ne specifica i presupposti; la relativa disciplina riprende quella dettata nell’art. 7 della direttiva 95/46/CE<sup>125</sup>.

Il trattamento è da considerarsi lecito “*nella misura in cui ricorre almeno una delle seguenti condizioni*”:

- Il consenso dell’interessato al trattamento;
- La destinazione del trattamento a specifiche finalità;
- La necessità del trattamento per:
  - L’esecuzione di un contratto di cui l’interessato è parte;
  - L’adempimento ad un obbligo legale cui è soggetto il titolare del trattamento;
  - La salvaguardia dell’interesse vitale dell’interessato;
  - Il perseguimento del legittimo interesse del titolare o di terzi.<sup>126</sup>

<sup>125</sup> Riccio G. M., Scorza G., Belisario E., *GDPR e Normativa Privacy – Commentario*, Wolters Kluwer, 2022, p. 85.

<sup>126</sup> Regolamento 2016/679, art. 6.



Deve essere ricondotto al già citato art. 52 della Carta di Nizza, che enuncia quanto segue nel par. 1<sup>127</sup>:

**Carta di Nizza – Art. 52, par. 1: Portata e interpretazione dei diritti e dei principi**

*1. Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.*

Dal quadro normativo delineato dal sopraccitato art. 8 CEDU, concernente il diritto al rispetto della propria vita privata e familiare e la protezione da ingerenze dell'autorità pubblica, nonché quanto disposto dall'art. 52 della Carta di Nizza, emerge la necessità di limitare l'ammissibilità delle operazioni di trattamento dei dati alle sole ipotesi in cui queste siano proporzionali, necessarie e funzionali al raggiungimento di uno scopo ben definito *ex lege*.

Ingerenze ulteriori, anche da parte di algoritmi IA, sarebbero giustificati esclusivamente in ipotesi eccezionali concernenti, ad esempio, la sicurezza nazionale o la pubblica sicurezza.

La giurisprudenza della Corte EDU ha in particolare delineato le ipotesi in cui il trattamento dei dati personali è da ritenersi legittimo, ossia:

- È conforme alla legge;
- Persegue uno scopo legittimo;
- È necessario in una società democratica per perseguire uno scopo legittimo.<sup>128</sup>

<sup>127</sup> Carta dei diritti fondamentali dell'Unione europea, 2000/C 364/01, art. 52, par. 1, [https://www.europarl.europa.eu/charter/pdf/text\\_it.pdf](https://www.europarl.europa.eu/charter/pdf/text_it.pdf)

<sup>128</sup> Riccio G. M., Scorza G., Belisario E., *GDPR e Normativa Privacy – Commentario*, Wolters Kluwer, 2022, p. 64.

Rileva con riguardo al principio della liceità anche il considerando 40, ai sensi del quale, affinché il trattamento di dati personali rispetti l'art. 5 GDPR, esso deve fondarsi sul *“consenso dell'interessato o su altra base legittima prevista per legge dal presente regolamento o dal diritto dell'Unione o degli Stati membri”*.<sup>129</sup> Un esempio di base giuridica del trattamento è la *“necessità di un contratto di cui l'interessato è parte o di esecuzione di misure precontrattuali adottate su richiesta dello stesso”*.<sup>130</sup>

Deve pertanto ritenersi che il principio di trasparenza debba essere considerato un elemento necessario per il consenso dell'interessato, non potendosi dire che il titolare abbia ottemperato a tali obblighi legali nell'ipotesi in cui la persona fisica sia sprovvista dell'informativa necessaria.

Rileva in tal senso anche il considerando 39 del GDPR, ai sensi del quale i dati personali dovrebbero essere *“adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento”*, e prevedendo che il titolare debba stabilire un termine per la *“cancellazione”* o la *“verifica periodica”* degli stessi.

---

<sup>129</sup> Regolamento 2016/679, Considerando 40.

<sup>130</sup> Bolognini L., Pelino E., Bistolfi C., *Il regolamento privacy europeo – Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè, 2016, p. 93.

Il Considerando 39 dispone quanto segue:

**Regolamento 2016/679 – Considerando 39:**

[...]

*Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati.*

*Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro.*

*Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano.*

*È opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento.*

*In particolare, le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali.<sup>131</sup>*

[...]

---

<sup>131</sup> Regolamento 2016/679, Considerando 39.

Il principio di trasparenza, dunque, attiene al contenuto delle informazioni oggetto del trattamento; in particolare, queste devono essere “facilmente accessibili e comprensibili”. Deve inoltre essere trasparente il *quomodo* del trattamento, ossia le modalità con cui i dati sono raccolti.

Dal dispositivo dell’art. 5 e del Considerando 39 emerge la necessità di garantire l’autodeterminazione informativa, cui il principio di trasparenza è funzionale: fornendo all’interessato le informazioni necessarie, questi è in grado di determinare le modalità del trattamento dei propri dati ed eventualmente esercitare il diritto di revoca previsto dal Regolamento.

Viene inoltre posta enfasi sulla sensibilizzazione delle persone alle caratteristiche essenziali del trattamento dei dati: in tal senso il GDPR pone numerosi obblighi in capo al titolare in termini di oneri comunicativi. Il principio di trasparenza è infatti complementare al principio di correttezza (dall’inglese *fairness*), essendo stato definito dal WP29 come espressione dello stesso e legato al principio di responsabilizzazione. Anche esso è strettamente legato alla già citata garanzia di autodeterminazione informativa, e concerne il rapporto tra il titolare e il responsabile del trattamento dei dati personali da un lato, e l’interessato dall’altro. In altre parole, il titolare del trattamento è tenuto ad agire in buona fede, evitando abusi del diritto.<sup>132</sup>

Nell’ambito dell’intelligenza artificiale, può dirsi a titolo esemplificativo che la profilazione a mezzo di processi automatizzati sia iniqua e dunque in violazione dei principi di trasparenza e correttezza nell’ipotesi in cui essa crei discriminazioni, ad esempio negando l’accesso a opportunità di lavoro o offrendo prodotti finanziari particolarmente rischiosi o costosi; alcuni consumatori potrebbero pertanto vedersi proposte offerte non rilevanti o meno interessanti rispetto ad altri.<sup>133</sup>

---

<sup>132</sup> Riccio G. M., Scorza G., Belisario E., *GDPR e Normativa Privacy – Commentario*, Wolters Kluwer, 2022, pp. 64-65

<sup>133</sup> Gruppo di Lavoro 29 per la protezione dei dati, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, 22 agosto 2018, p. 10, [http://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=612053](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053).

Rileva in tal senso anche il Considerando 60, ai sensi del quale *“i principi di trattamento corretto e trasparente implicano che l’interessato sia informato dell’esistenza del trattamento e delle sue finalità”*; inoltre, *“l’interessato dovrebbe essere informato dell’esistenza di una profilazione e delle conseguenze della stessa”*<sup>134</sup>. Il Considerando 71 statuisce inoltre che è opportuno al fine di garantire il rispetto dei principi di trattamento corretto e trasparente che il titolare *“utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate”*<sup>135</sup>.

### 3.3 Il consenso dell’interessato

Prima di procedere all’analisi delle possibili forme di trattamento dei dati personali anche a mezzo di algoritmi, occorre analizzare gli artt. 4, comma I, n. 11 e 7 del Regolamento, concernenti il consenso dell’interessato:

#### **Regolamento 2016/679 – Articolo 4: Definizioni**

*11) «consenso dell’interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell’interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;*

<sup>134</sup> Regolamento 2016/679, Considerando 60.

<sup>135</sup> Regolamento 2016/679, Considerando 71.

## **Regolamento 2016/679 – Articolo 7: Condizioni per il consenso**

*1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.*

[...]

*3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.*

*4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.<sup>136</sup>*

Il consenso dell'interessato così delineato può definirsi come una delle condizioni del principio di liceità previamente analizzato. La nozione fornita dall'art. 4 del Regolamento riprende quella della Direttiva 95/46/CE, ove il consenso era definito come “*qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di trattamento*”<sup>137</sup>.

<sup>136</sup> Regolamento 2016/679, art. 4 n. 11, e art. 7.

<sup>137</sup> Direttiva 95/46/CE, art. 2, paragrafo 1, lettera h), <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:31995L0046&from=EL>.

In particolare, affinché il consenso sia valido, esso dovrà presentare le seguenti caratteristiche:

- **Informato:** l'interessato deve conoscere in modo chiaro e intellegibile:
  - Le modalità e finalità del trattamento;
  - Le conseguenze del suo assenso o diniego;
  - Eventuali informazioni ulteriori per una scelta consapevole.
- **Libero:** l'interessato deve avere una scelta effettiva ed il controllo sui propri dati personali.
- **Specifico:** il consenso dell'interessato deve essere espresso in relazione a specifiche finalità, mantenendo la possibilità di scegliere separatamente in relazione ad esse.
- **Inequivocabile:** il consenso deve essere manifestato in modo ovvio e attivo dall'interessato con un'azione deliberata.
- **Dimostrabile:** il titolare deve essere in grado di dimostrare la manifestazione del consenso da parte dell'interessato.
- **Revocabile:** l'interessato deve avere il diritto di revocare il consenso facilmente e in qualsiasi momento.
- **Espresso / esplicito:** deve consistere in una dichiarazione esplicita di volontà.<sup>138</sup>

---

<sup>138</sup> Cassano G., Colarocco V., Gallus G. B., Micozzi F. P., *Il processo di adeguamento al GDPR*, Giuffrè, 2022.

### 3.4 La profilazione e pseudonimizzazione

La profilazione costituisce una delle forme concrete di applicazione del trattamento automatizzato e, in quanto tale, rileva particolarmente nell'ambito dell'intelligenza artificiale. Essa è così definita nel Regolamento:

#### **Regolamento 2016/679 – Articolo 4: Definizioni**

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

L'articolo fa in questo caso esplicito riferimento al solo trattamento automatizzato. Trattasi specificamente di una “*tecnica di trattamento automatico mediante algoritmi di molteplici tipologie di dati personali relativi a quantità numericamente elevatissime di persone, per attribuire a ciascuna di queste ultime un profilo, ovvero una categoria predefinita e delineata attraverso parametri che il responsabile del trattamento considera necessari alla sua ricerca, al raggiungimento del suo scopo; il target è studiato nelle sue abitudini di consumo e negli stili di vita che ne rivelano attitudine e capacità di spesa, gusti per alcuni prodotti o servizi e disinteresse per altri, caratteristiche legate alla sua identità personale*”.<sup>139</sup>

Emergono in questa prospettiva le possibilità di applicazione degli algoritmi di intelligenza artificiale, a mezzo dei quali è possibile realizzare sistemi di aggregazione in *cluster*. Questi consistono in tecniche di incrocio ed associazione di dati personali degli utenti con le informazioni elaborate dagli algoritmi, consentendo di identificare con più precisione le

---

<sup>139</sup> Pacileo, *Profilazione e diritto di opposizione*, in Sica-D'Antonio-Riccio, *La Nuova Disciplina Europea della Privacy*, pp. 177-196.



persone fisiche oggetto del trattamento; queste, dunque, sono inserite in categorie omogenee.<sup>140</sup> In generale, la profilazione consiste in due tipi di processi: la creazione di un profilo a partire dalle caratteristiche di una o più persone, e l'applicazione del profilo in questione in base alle informazioni e caratteristiche così elaborate.<sup>141</sup>

Poiché la profilazione non è un processo immediatamente percepibile da chi lo subisce, il legislatore europeo ha stabilito nell'art. 12, par. 1 del Capo III, sezione I<sup>142</sup>, concernente i diritti dell'interessato e, specificamente, la trasparenza e le modalità del trattamento, quanto segue:

**Regolamento 2016/679 - Articolo 12: Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato**

*1. Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni [...] relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. [...]*

Le informazioni concernenti la profilazione devono pertanto essere fornite in forma “*concisa, trasparente, intelligibile e facilmente accessibile*”, nonché con un “*linguaggio semplice e chiaro*”, in accordo con i tre principi ex art. 5 GDPR precedentemente esaminati.

La pseudonimizzazione è un'ulteriore modalità del trattamento dei dati personali. La norma non fa in questo caso riferimento al solo trattamento automatizzato, rendendola dunque applicabile anche alle ipotesi di intervento umano.

<sup>140</sup> Pizzetti F., *Privacy e Diritto europeo della protezione dei dati personali. Dalla Direttiva 95/46 al Nuovo Regolamento Europeo*, I Diritti nella “rete” della rete, Torino, 2016, pp. 6-19; 23-35; 175-177, 182-196.

<sup>141</sup> Kuner, Christopher and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary (New York, 2020; online edn, Oxford Academic)*, 13 febbraio 2020, <https://doi.org/10.1093/oso/9780198826491.001.0001>; Hildebrandt 2008, p. 19; WP29 2018, p. 7.

<sup>142</sup> Regolamento 2016/679, art. 12.

Essa è definita come segue:

#### **Regolamento 2016/679 – Articolo 4: Definizioni**

5) «pseudonimizzazione»: *il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;*

Saranno pertanto necessarie informazioni aggiuntive al fine di ricondurre i dati personali alle persone fisiche destinatarie del trattamento dei dati. Come suggerito dal Considerando 28, tali tecniche hanno lo scopo di ridurre i rischi che possono incidere sui diritti degli interessati, nonché facilitare il rispetto degli obblighi di protezione dei dati in capo ai titolari ed ai responsabili del trattamento dei dati.<sup>143</sup>

La pseudonimizzazione consiste nell'uso di tecniche volte a sostituire dati identificativi personali all'interno di un set di dati, quali ad esempio il nome o la data di nascita, con un attributo diverso, come un codice assegnato in modo casuale<sup>144</sup>.

Al termine del processo l'interessato sarà ancora indirettamente identificabile, e i dati sottoposti al processo di pseudonimizzazione saranno comunque inquadrabili come dati personali.<sup>145</sup> Le informazioni aggiuntive menzionate nell'articolo necessarie alla re-identificazione dell'interessato, quali ad esempio chiavi di crittografia, dovranno inoltre essere conservate separatamente.

---

<sup>143</sup> Tosoni L., 'Article 4(5). Pseudonymisation', in Kuner C. and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (New York, 2020; online edn, Oxford Academic), 13 febbraio 2020, <https://doi.org/10.1093/oso/9780198826491.003.0011>

<sup>144</sup> WP29 2007, *Opinion 4/2007 on the concept of personal data*, 20 giugno 2007, p. 18, [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf).

<sup>145</sup> WP29 2014, *Opinion 05/2014 on Anonymisation Techniques*, 10 aprile 2014, p. 20, [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf).

Ai sensi del Considerando 29, la separazione in questione può avvenire anche “*all'interno dello stesso titolare del trattamento, qualora il titolare del trattamento abbia adottato le misure tecniche e organizzative necessarie ad assicurare, per il trattamento interessato, l'attuazione del presente regolamento*”<sup>146, 147</sup>.

In alcuni casi, la minimizzazione dei dati menzionata nell'art. 25 GDPR potrebbe richiedere la riduzione delle informazioni che rendono possibile identificare un individuo, piuttosto che la quantità di dati stessi. Ciò potrebbe essere ottenuto attraverso la pseudonimizzazione, che riduce la facilità di associare i dati a una persona specifica.<sup>148</sup>

### 3.5 Il titolare e il responsabile del trattamento

Il titolare del trattamento dei dati personali (“*controller*”) e il relativo responsabile (“*processor*”) sono definiti come segue:

#### **Regolamento 2016/679 – Articolo 4: Definizioni**

7) «*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;

8) «*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;

<sup>146</sup> Regolamento 2016/679, Considerando 29.

<sup>147</sup> Tosoni L, 'Article 4(5). Pseudonymisation', in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (New York, 2020; online edn, Oxford Academic), 13 febbraio 2020, <https://doi.org/10.1093/oso/9780198826491.003.0011>.

<sup>148</sup> European Parliamentary Research Service, Scientific Foresight Unit (STOA), PE 641.530, *The impact of the General Data Protection Regulation (GDPR) on Artificial intelligence*, giugno 2020, p. 49, [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS\\_STU\(2020\)641530\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf).

L'art. 4 fornisce anche una nozione di rappresentante, ossia la persona designata dalle figure sopraccitate con lo scopo di rappresentarle nell'ambito del rispetto dei rispettivi obblighi a norma del Regolamento.

Il Considerando 74 stabilisce a riguardo che il titolare del trattamento ha il compito di dimostrare la conformità delle attività di trattamento poste in essere con quanto disposto dal GDPR, ponendo particolare enfasi sulla “efficacia delle misure, l'ambito di applicazione, il contesto e le finalità del trattamento”, nonché il “rischio per i diritti e le libertà delle persone fisiche”.<sup>149</sup>

Sebbene l'articolo menzioni la possibilità che il titolare sia una persona fisica, trattasi generalmente di un'organizzazione con il compito di delineare gli aspetti essenziali del trattamento, quali gli scopi e i mezzi. In particolare, la *European Data Protection Board* (EDBP) ha stabilito<sup>150</sup> che non sussistano limitazioni per quanto concerne la natura dell'entità che svolge il ruolo di titolare del trattamento.

Rileva inoltre la sentenza della Corte di Giustizia nel caso *Wirtschaftsakademie*<sup>151</sup>, ove è stato precisato che non sia necessaria per il titolare la possibilità di accedere ai dati trattati: è sufficiente che la persona fisica o giuridica sia in grado di esercitare un'influenza determinante sulle finalità ed i mezzi essenziali del trattamento al fine di qualificarla come titolare del trattamento ex art. 4 GDPR.<sup>152</sup>

Il titolare è pertanto il centro di imputazione delle concernenti i mezzi e le finalità sinora menzionate, e il ruolo dipende dal potere decisorio concretamente, prescindendo da eventuali diverse qualificazioni formali. Possono essere previsti casi di titolarità ex lege.

---

<sup>149</sup> Regolamento 2016/679, Considerando 74.

<sup>150</sup> EDBP, *Linee Guida 07/2020*, Versione 2.0 – adottate il 7 luglio 2021 in seguito a consultazione pubblica, [https://edpb.europa.eu/system/files/2022-02/eppb\\_guidelines\\_202007\\_controllerprocessor\\_final\\_it.pdf](https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_it.pdf)

<sup>151</sup> C-210/16, Corte di Giustizia, *Wirtschaftsakademie*, <https://curia.europa.eu/juris/document/document.jsf?jsessionid=26C8105924103B17DBBD79E27C879B37?text=&docid=202543&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=877225>

<sup>152</sup> Riccio G. M., Scorza G., Belisario E., *GDPR e Normativa Privacy – Commentario*, Wolters Kluwer, Ed. II, 2022, pp. 49-50

La dottrina sul GDPR suggerisce che le funzioni del titolare possano essere raggruppate in tre categorie: obblighi e adempimenti in materia di sicurezza, di garanzia nei confronti dell'interessato, di collaborazione con soggetti preposti al controllo.

Per quanto concerne il profilo della sicurezza, il titolare ha il compito di decidere e programma misure appropriate allo scopo. L'art. 25 del GDPR stabilisce in tal senso che il titolare debba mettere in atto “*misure tecniche e organizzative adeguate*” sia prima ancora che i mezzi del trattamento siano stati determinati (ossia nella fase di progettazione: trattasi in questo caso di *privacy by design*), sia nel corso del trattamento stesso (delineandosi pertanto un obbligo di aggiornarle progressivamente). Il titolare dovrà tenere conto di numerosi fattori, quali:

- Lo stato dell'arte;
- I costi dell'attuazione;
- La natura e l'ambito di applicazione;
- Il contesto e le finalità del trattamento;
- I rischi concernenti i diritti e le libertà delle persone fisiche.

Con riguardo ai mezzi utilizzati, il titolare deve anche operare una valutazione d'impatto sulla protezione dei dati: il GDPR non menziona esplicitamente l'intelligenza artificiale, ma riconosce che l'uso di “*nuove tecnologie*” possa comportare dei rischi con “*probabilità e gravità diverse per i diritti e le libertà delle persone fisiche*”. Una volta determinato il *modus operandi*, il titolare sarà tenuto ad attuare le misure di sicurezza in questione.

Il titolare dovrà inoltre conformarsi ai principi di trasparenza e responsabilizzazione, e designare nei casi previsti dalla legge la figura del *data protection officer*, con il quale collabora, fornendo il necessario per realizzare la sua attività<sup>153</sup>.<sup>154</sup>

---

<sup>153</sup> Regolamento 2016/679, art. 38.

<sup>154</sup> Bolognini L., Pelino E., Bistolfi C., *Il regolamento privacy europeo – Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè, 2016, p. 121.

Occorre sottolineare come la Corte di Giustizia dell'Unione Europea abbia precisato che il concetto di titolare debba essere inteso in modo generale, in modo da consentire una protezione effettiva e completa dei dati degli interessati.<sup>155</sup>

La figura del responsabile svolge un ruolo di rilevanza sempre maggiore in seguito ai recenti sviluppi nel campo organizzativo e tecnologico, nonché nella tendenza all'affidare la gestione dei processi di trattamento dei dati a soggetti esterni; in particolare, i fornitori di servizi cloud svolgono spesso il ruolo di responsabili del trattamento. L'articolo 28 del GDPR ne specifica le funzioni come segue:

#### **Regolamento 2016/679 – Articolo 28: Responsabile del trattamento**

*1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.*

Il responsabile del trattamento svolge pertanto il trattamento in base alle finalità delineate dal titolare; la sua attività ha natura principalmente strumentale rispetto alle funzioni di quest'ultimo. La figura deve presentare “*garanzie sufficienti*” allo scopo di porre in essere le misure tecniche e organizzative precedentemente menzionate.<sup>156</sup>

---

<sup>155</sup> Caso C-131/12, *Google Spain*, para. 34; Caso C-210/16, *Wirtschaftsakademie*, para. 28; Caso C-40/17, *Fashion ID*, parag. 65–66.

<sup>156</sup> Riccio G. M., Scorza G., Belisario E., *GDPR e Normativa Privacy – Commentario*, Wolters Kluwer, 2022, pp. 342-343.

L'European Data Protection Board ha precisato che sussistono alcune condizioni per qualificare un soggetto come responsabile del trattamento:

1. Deve trattarsi di un soggetto separato dal titolare del trattamento;
2. Il trattamento deve avvenire per conto del titolare;
3. Il responsabile deve trattare i dati entro i limiti delle modalità e finalità delineate dal titolare del trattamento.<sup>157</sup>

Dunque, il responsabile del trattamento ha meramente lo scopo di seguire le direttive fornite del titolare, e sarebbe esso stesso qualificabile come tale nell'ipotesi in cui configurasse autonomamente le modalità e finalità del trattamento. Va inoltre sottolineato come il responsabile sia un'entità legalmente distinta dal titolare del trattamento, sebbene quest'ultimo possa svolgere le relative operazioni sui dati personali autonomamente. Al contrario<sup>158</sup>.

L'articolo 28.10 del GDPR chiarisce ulteriormente il punto stabilendo che *“se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione”*.<sup>159</sup> Il WP29 ha anche precisato che il responsabile che *“acquisisce un ruolo rilevante nella determinazione delle finalità o degli aspetti fondamentali dei mezzi del trattamento”* assume il ruolo di contitolare.<sup>160</sup>

---

<sup>157</sup> European Data Protection Board, *Linee Guida 7/2020*, Versione 2.0 - adottate il 7 luglio 2021 in seguito a consultazione pubblica, [https://edpb.europa.eu/system/files/2022-02/eppb\\_guidelines\\_202007\\_controllerprocessor\\_final\\_it.pdf](https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_it.pdf).

<sup>158</sup> Bygrave, Lee A., e Tosoni L., *'Article 4(8). Processor'*, in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (New York, 2020; online edn, Oxford Academic), 13 febbraio 2020, <https://doi.org/10.1093/oso/9780198826491.003.0014>.

<sup>159</sup> Regolamento 2016/679, art. 28.

<sup>160</sup> WP29, *Opinion 1/2010 on the concepts of "controller" and "processor"*, 16 febbraio 2010, [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf).

### 3.6 Il processo decisionale automatizzato e l'intervento umano

L'articolo 22 del Regolamento contiene le disposizioni di maggior rilievo per quanto concerne l'intelligenza artificiale, poiché tratta in modo approfondito il processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione sopra esaminata.

La norma presenta spunti di rilievo dal punto di vista storico-giuridico. La Commissione europea si espresse già nel 1990 con riguardo ai processi decisionali automatizzati nel contesto dell'Articolo 15 della Direttiva 95/46/CE (concernente il medesimo argomento). Essa stabilì come lo scopo della norma fosse quello di tutelare l'interesse dei destinatari del trattamento, specie con riguardo all'adozione di decisioni con effetti in grado di incidere sulle loro sfere giuridiche. In particolare, la Commissione pose enfaticamente l'intenzione di evitare che grandi istituzioni pubbliche o private prendessero le decisioni in esame sulla base della sola "data shadow"<sup>161</sup> degli interessati.<sup>162</sup>

Nel 1992 la Commissione approfondì ulteriormente la questione, focalizzandosi sui potenziali pericoli derivanti dall'utilizzo improprio degli strumenti di trattamento dei dati nell'ambito del processo decisionale. In particolare, essa suggerì che i risultati prodotti dagli algoritmi a mezzo di software avanzati e sistemi esperti, oggi generalmente inquadrabili come intelligenze artificiali, avrebbero potuto indurre il *decision-maker* umano a farvi eccessivo affidamento, riducendone sempre più lo spazio per l'intervento e le relative responsabilità.

In tal senso l'articolo 16.1 della Direttiva 95/46/CE stabiliva un importante principio: l'interessato non sarebbe stato obbligato ad accettare la decisione di una pubblica

---

<sup>161</sup> Proposta di direttiva del Consiglio concernente la protezione delle persone relativamente al trattamento dei dati personali, presentata dalla Commissione il 27 luglio 1990, p. 29, [https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:51990PC0314\(01\)&from=en](https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:51990PC0314(01)&from=en).

<sup>162</sup> Bygrave, Lee A, 'Article 22 Automated individual decision-making, including profiling', in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (New York, 2020; online edn, Oxford Academic), 13 febbraio 2020, <https://doi.org/10.1093/oso/9780198826491.003.0055>.



amministrazione o di un ente privato con effetti in grado di incidere la sfera giuridica, nell'ipotesi in cui il relativo processo decisionale fosse del tutto automatizzato.<sup>163</sup>

I contenuti dell'articolo 15 della Direttiva 95/46/CE sono traslati nel sopraccitato art. 22 del GDPR. La normativa vigente dispone quanto segue:

**Regolamento 2016/679 – Articolo 22: Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione**

1. *L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.*
2. *Il paragrafo 1 non si applica nel caso in cui la decisione:*
  - a) *sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;*
  - b) *sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;*
  - c) *si basi sul consenso esplicito dell'interessato.*
3. *Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.*
4. *Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.<sup>164</sup>*

<sup>163</sup> Commission of the European Communities, *Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, 15 ottobre 1992, p. 26, <https://aei.pitt.edu/10375/1/10375.pdf>.

<sup>164</sup> Regolamento 2016/679, art. 22.

L'articolo sancisce l'importante diritto dell'interessato a non essere sottoposto a decisioni basate sul solo trattamento automatizzato.

In particolare, la disposizione contenuta nell'art. 22.1 comporta importanti ripercussioni sull'utilizzo dell'intelligenza artificiale come delineata nei capitoli precedenti. Trattandosi di algoritmi in grado di operare su enormi quantità di dati, questi si prestano all'utilizzo nel campo della profilazione, elaborando categorie omogenee di soggetti.

Il Regolamento stabilisce tuttavia che, prescindendo dagli sviluppi nel campo della tecnologia, la sfera giuridica degli interessati non potrà in alcun modo essere incisa dalla sola intelligenza artificiale, salvo questi non vi consentano esplicitamente. Sulla base dei principi di liceità e trasparenza sopraccitati, dunque, i destinatari del trattamento dovranno ricevere informazioni sufficienti concernenti il processo decisionale automatizzato che li riguarda.

Il Considerando 71 fornisce degli esempi di effetti giuridici riguardanti l'interessato o in grado di incidere significativamente sulla sua persona, citando *“il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani”*. Esso ribadisce anche la necessità di subordinare il trattamento a *“garanzie adeguate”*, comprensive delle informazioni da fornire all'interessato, nonché del diritto di ottenere l'intervento umano.

Il considerando fa inoltre riferimento ai già citati processi di profilazione, definendoli a sua volta come *“forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti”* di natura eterogenea.<sup>165</sup>

La profilazione così definita a mezzo di processi automatizzati, e quindi di algoritmi di AI sempre più efficienti in ragione dei traguardi raggiunti nel campo tecnologico, è oggi diffusa in numerosi settori; ciò ha tuttavia comportato parallelamente un aumento significativo dei rischi per i diritti e le libertà degli individui connessi al loro utilizzo.

---

<sup>165</sup> Regolamento 2016/679, Considerando 71.

Si utilizza in tale contesto la nozione di *black box society* in riferimento all'opacità dei processi decisionali automatizzati, dei quali gli individui non sono al corrente, o non potrebbero comprendere appieno per via della grande complessità degli algoritmi utilizzati e del *machine learning*, come si è più volte enfatizzato nel Capitolo I della presente trattazione.<sup>166</sup>

La profilazione, come evidenziato dal WP29, può comportare discriminazioni degli individui ove sussistano imperfezioni nell'istruzione degli algoritmi; trattasi in tali ipotesi di *bias* dell'intelligenza artificiale.

Occorre precisare la nozione di *bias cognitivi*, ossia i preconcetti e le convinzioni alla base delle decisioni prese dall'uomo che ne condizionano l'analisi delle informazioni, creando delle abitudini potenzialmente errate. Poiché gli algoritmi sono progettati da esseri umani, l'intelligenza artificiale si presterà al medesimo errore, poiché analizza con approccio statico quantità sempre più grandi di dati. Occorre citare nuovamente anche il concetto di *deep learning*, che consente di istruire le reti neurali, ispirate al funzionamento del cervello umano, a mezzo di algoritmi.

Per facilitare la comprensione del tecnicismo in esame, è sufficiente utilizzare come esempio i sistemi di riconoscimento facciale. Quando questi sono soggetti a *bias*, il pregiudizio esistente nel sistema è stato ignorato, oppure il costante aumento della quantità di dati analizzati dagli algoritmi ha progressivamente nascosto l'errore sempre più in profondità nel codice. IBM ha tentato di ovviare al problema e ridurre l'errore nel proprio sistema realizzando un *data set* denominato *Diversity in Face*, composto da 1 milione di immagini e 10 schemi di codifica. Facebook ha utilizzato per il proprio sistema *Deep Face*, realizzato nel 2014, una base composta da un *set* provvisto di 120 milioni di parametri divisi in 9 livelli di dettaglio volti all'utilizzo su 4 milioni di foto, oggi decuplicate.<sup>167</sup>

---

<sup>166</sup> Riccio G. M., Scorza G., Belisario E., *GDPR e Normativa Privacy – Commentario*, Wolters Kluwer, 2022, p. 280.

<sup>167</sup> Agenda Digitale, Giribaldi D., *Intelligenza artificiale, tutti i pregiudizi (bias) che la rendono pericolosa*, 26 febbraio 2019, <https://www.agendadigitale.eu/cultura-digitale/intelligenza-artificiale-tutti-i-pregiudizi-bias-che-la-rendono-pericolosa/>.

## CAPITOLO IV

### La Proposta di Regolamento dell'Unione Europea in materia di intelligenza artificiale

#### 4.1 Riflessioni sui motivi e obiettivi della proposta

La proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale<sup>168</sup> è di rilevanza fondamentale per la presente trattazione, costituendo essa uno dei più recenti sviluppi nel contesto giuridico per quanto concerne i sistemi di IA.

Al tempo della stesura della presente trattazione, la proposta di regolamento è stata definita anche come “*AI Act*”<sup>169</sup>, e concerne la prima potenziale legge specificamente concernente il settore dell'intelligenza artificiale, suddividendone i relativi sistemi in tre categorie che saranno esaminate approfonditamente.

La proposta delinea a titolo introduttivo i seguenti obiettivi specifici:

- *Assicurare che i sistemi di IA immessi sul mercato dell'Unione e utilizzati siano sicuri e rispettino la normativa vigente in materia di diritti fondamentali e i valori dell'Unione;*
- *Assicurare la certezza del diritto per facilitare gli investimenti e l'innovazione nell'intelligenza artificiale;*
- *migliorare la governance e l'applicazione effettiva della normativa esistente in materia di diritti fondamentali e requisiti di sicurezza applicabili ai sistemi di IA;*
- *facilitare lo sviluppo di un mercato unico per applicazioni di IA lecite, sicure e affidabili nonché prevenire la frammentazione del mercato.*<sup>170</sup>

<sup>168</sup> Commissione Europea, *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislative dell'Unione*, 21 aprile 2021, <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021PC0206&from=IT>

<sup>169</sup> The Artificial Intelligence Act, <https://artificialintelligenceact.eu/>

<sup>170</sup> AI Act, p. 3.

La proposta menziona in tal senso le richieste del Parlamento europeo e del Consiglio europeo, che concernevano la necessità di un intervento legislativo volto a garantire il “*funzionamento del mercato interno per i sistemi di IA*”.<sup>171</sup> Il Regolamento proposto ha infatti lo scopo di stabilire “*regole armonizzate sull’intelligenza artificiale*”.

Come precedentemente osservato, il Regolamento Generale per la Protezione dei Dati non definisce mai tali tecnologie in modo diretto negli artt. 4 e 22; la normativa vigente si limita a fornire nozioni di natura generale sul processo decisionale automatizzato, nonché i principi cui i relativi strumenti devono adeguarsi. Il legislatore ha così tenuto conto degli sviluppi futuri nel campo della protezione dei dati personali, ricomprendendo però solo indirettamente gli odierni sistemi di intelligenza artificiale, i quali, come si è evidenziato, hanno raggiunto un livello di complessità e autonomia tale da necessitare di una regolamentazione *ad hoc*.

La proposta concerne i moderni sistemi di intelligenza artificiale, e fornisce numerose definizioni che saranno esaminate approfonditamente. Essa definisce l’intelligenza artificiale (IA) come “*una famiglia di tecnologie in rapida evoluzione in grado di apportare una vasta gamma di benefici economici e sociali in tutto lo spettro delle attività industriali e sociali*”.

La proposta prevede l’uso dell’IA in diversi settori di particolare rilevanza, specie con riguardo a quelli dei “*cambiamenti climatici, dell’ambiente e della sanità, il settore pubblico, la finanza, la mobilità, gli affari interni e l’agricoltura*” allo scopo di trarne numerosi vantaggi e benefici, tra cui:

- Il miglioramento delle previsioni;
- L’ottimizzazione delle operazioni;
- L’ottimizzazione dell’assegnazione delle risorse;
- La personalizzazione dell’erogazione di servizi;
- I vantaggi che l’IA può comportare dal punto di vista sociale e ambientale;
- I vantaggi competitivi fondamentali che può fornire alle imprese e all’economia europea.<sup>172</sup>

---

<sup>171</sup> AI Act, p. 2.

<sup>172</sup> AI Act, p. 1.

La proposta cita il duplice obiettivo del Libro Bianco sull'intelligenza artificiale<sup>173</sup> di promuovere l'adozione dell'IA affrontando i rischi associati all'utilizzo di tale tecnologia, prefiggendosi lo scopo di attuare il secondo, onde sviluppare un “*ecosistema di fiducia proponendo un quadro giuridico per un'IA affidabile*”.<sup>174</sup>

Da un punto di vista generale la proposta statuisce, dunque, che la regolamentazione europea dell'IA deve essere equilibrata e proporzionata, evitando di limitare eccessivamente lo sviluppo delle nuove tecnologie, citando contestualmente i rischi che possono derivare da determinati utilizzi dei moderni sistemi di intelligenza artificiale.

Il quadro giuridico concernente l'intelligenza artificiale dovrà garantire che tali sistemi siano utilizzati nel rispetto dei valori dell'Unione Europea, nonché del diritto attualmente vigente, nonché assicurare che i cittadini europei siano in grado di beneficiare delle nuove tecnologie di IA senza rinunciare ai valori e i principi che caratterizzano il sistema giuridico comune.

La Commissione europea ha condotto una valutazione d'impatto concernente la proposta in esame, al fine di delineare le opzioni strategiche relative ai diversi gradi di intervento più appropriate. La valutazione in questione si è conclusa con un parere positivo del comitato per il controllo normativo in data 21 marzo 2021.

---

<sup>173</sup> Commissione europea, , *Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia* (COM(2020) 65 final), 19 febbraio 2020.

<sup>174</sup> AI Act, p. 1.

Seguono le opzioni considerate:

*Opzione 1: strumento legislativo dell'UE che istituisce un sistema di etichettatura volontario;*

*Opzione 2: approccio settoriale "ad hoc";*

*Opzione 3: strumento legislativo orizzontale dell'UE che segue un approccio proporzionato basato sul rischio;*

*Opzione 3+: strumento legislativo orizzontale dell'UE che segue un approccio proporzionato basato sul rischio + codici di condotta per i sistemi di IA non ad alto rischio;*

*Opzione 4: strumento legislativo orizzontale dell'UE che stabilisce requisiti obbligatori per tutti i sistemi di IA, indipendentemente dal rischio che pongono.<sup>175</sup>*

La proposta è basata sull'opzione 3+, che prevede un quadro normativo soltanto per i sistemi di IA ad alto rischio, con la possibilità per tutti i fornitori di sistemi di IA non ad alto rischio di seguire un codice di condotta.

Riassumendone i punti principali, la proposta mira pertanto a:

- Proteggere i diritti fondamentali delle persone, inclusi i diritti alla privacy e alla protezione dei dati, nonché a prevenire la discriminazione e l'aggravamento delle disuguaglianze.
- Promuovere l'innovazione, la competitività e la crescita economica in Europa, fornendo un quadro chiaro e coerente per l'uso dell'IA.
- Garantire la sicurezza pubblica e la tutela della salute e dell'ambiente.
- La previsione di requisiti obbligatori per i sistemi di IA ad alto rischio concernenti i “dati, la documentazione e la tracciabilità, la fornitura di informazioni e la trasparenza, la sorveglianza umana, la robustezza e la precisione”.

---

<sup>175</sup> AI Act, p. 10.

Per raggiungere questi obiettivi, la proposta di regolamento stabilisce regole per l'uso dell'IA in una serie di settori, tra cui l'automazione industriale, i trasporti, la sanità, la sicurezza pubblica e la gestione dei dati. Inoltre, la proposta prevede l'istituzione di un sistema di valutazione della conformità e di sorveglianza per garantire il rispetto delle regole da parte delle imprese che sviluppano e utilizzano l'IA.

La proposta, dunque, promuove l'uso sicuro e responsabile dei tali sistemi al fine di massimizzarne i benefici, e contribuisce all'obiettivo dell'Unione europea di esser un “*leader mondiale nello sviluppo di un'intelligenza artificiale sicura, affidabile ed etica*”. La proposta prevede inoltre l'istituzione di un comitato europeo per l'intelligenza artificiale.

Al tempo della stesura della presente trattazione è possibile menzionare a titolo esemplificativo, onde comprendere appieno l'entità dei traguardi raggiunti dai sistemi di IA, il prototipo di chatbot ChatGPT<sup>176</sup> (*Chat Generative Pre-trained Transformer*). Sviluppato da OpenAI e rilasciato al pubblico il 30 novembre 2022, il software sfrutta sistemi di intelligenza artificiale e *machine learning*, ed è programmato per conversare con un utente umano. Il modello è addestrato sull'infrastruttura di *supercomputing* sviluppata da Microsoft denominata Azure AI, ed il relativo *dataset* include circa 300 miliardi di parole provenienti da libri, *webtext*, Wikipedia ed articoli disponibili su internet.<sup>177</sup>

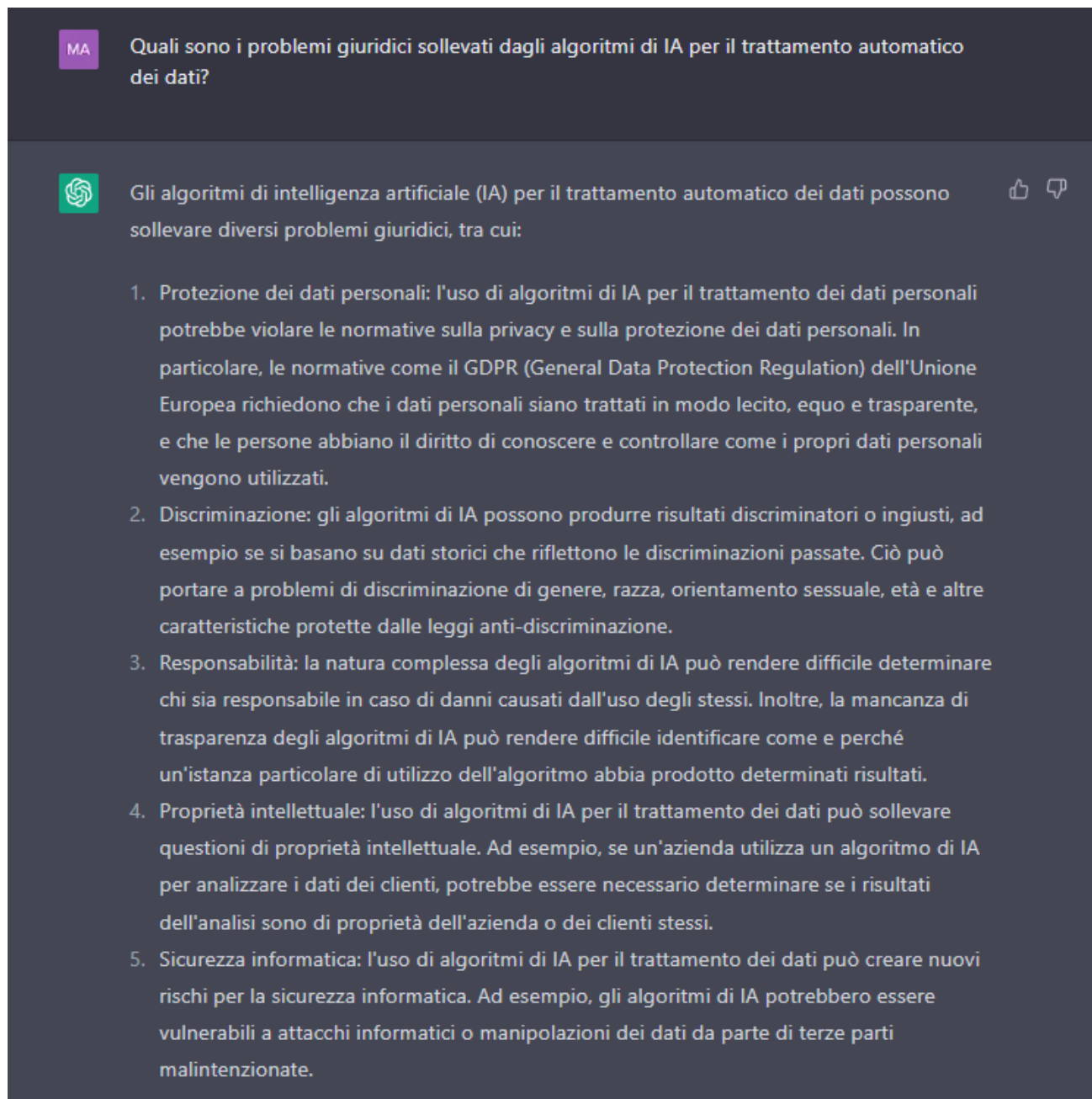
---

<sup>176</sup> OpenAI, *ChatGPT: Optimizing Language Models for Dialogue*, 30 novembre 2022, <https://openai.com/blog/chatgpt/>

<sup>177</sup> Hughes A., *ChatGPT: Everything you need to know about OpenAI's GPT-3 tool*, 2 febbraio 2023, <https://www.sciencefocus.com/future-technology/gpt-3/>



Segue un esempio di conversazione con ChatGPT<sup>178</sup> concernente l'oggetto della presente trattazione:



MA Quali sono i problemi giuridici sollevati dagli algoritmi di IA per il trattamento automatico dei dati?

Gli algoritmi di intelligenza artificiale (IA) per il trattamento automatico dei dati possono sollevare diversi problemi giuridici, tra cui:

1. Protezione dei dati personali: l'uso di algoritmi di IA per il trattamento dei dati personali potrebbe violare le normative sulla privacy e sulla protezione dei dati personali. In particolare, le normative come il GDPR (General Data Protection Regulation) dell'Unione Europea richiedono che i dati personali siano trattati in modo lecito, equo e trasparente, e che le persone abbiano il diritto di conoscere e controllare come i propri dati personali vengono utilizzati.
2. Discriminazione: gli algoritmi di IA possono produrre risultati discriminatori o ingiusti, ad esempio se si basano su dati storici che riflettono le discriminazioni passate. Ciò può portare a problemi di discriminazione di genere, razza, orientamento sessuale, età e altre caratteristiche protette dalle leggi anti-discriminazione.
3. Responsabilità: la natura complessa degli algoritmi di IA può rendere difficile determinare chi sia responsabile in caso di danni causati dall'uso degli stessi. Inoltre, la mancanza di trasparenza degli algoritmi di IA può rendere difficile identificare come e perché un'istanza particolare di utilizzo dell'algoritmo abbia prodotto determinati risultati.
4. Proprietà intellettuale: l'uso di algoritmi di IA per il trattamento dei dati può sollevare questioni di proprietà intellettuale. Ad esempio, se un'azienda utilizza un algoritmo di IA per analizzare i dati dei clienti, potrebbe essere necessario determinare se i risultati dell'analisi sono di proprietà dell'azienda o dei clienti stessi.
5. Sicurezza informatica: l'uso di algoritmi di IA per il trattamento dei dati può creare nuovi rischi per la sicurezza informatica. Ad esempio, gli algoritmi di IA potrebbero essere vulnerabili a attacchi informatici o manipolazioni dei dati da parte di terze parti malintenzionate.

L'esempio fornito offre alcuni spunti di riflessione per quanto concerne le ragioni che hanno indotto l'Unione a ritenere necessaria l'adozione del Regolamento oggetto della proposta.

---

<sup>178</sup> Le risposte del chatbot sono fornite in tempo reale, e si basano interamente sull'ampio *dataset* utilizzato per addestrarne il relativo modello. Sebbene esso non sia in grado di fornire pareri giuridici in grado di soddisfare gli standard qualitativi che il professionista umano può garantire, è possibile osservare come il chatbot abbia correttamente individuato alcune delle potenziali problematiche scaturenti dall'uso dei sistemi di IA nell'ambito della protezione dei dati.

Considerando gli odierni sistemi di IA, quali quelli di riconoscimento facciale menzionati in riferimento al processo decisionale automatizzato *ex art. 22 GDPR*, nonché la capacità di software quali ChatGPT di fornire informazioni su qualsiasi argomento a mezzo di un'interfaccia *user-friendly*, e in particolare la rapida evoluzione di tali strumenti, si comprende appieno la necessità dell'intervento legislativo prospettato dal Parlamento e dal Consiglio, al fine di affrontare i rischi insiti nella rivoluzione tecnologica in atto a mezzo di strumenti normativi adeguati, garantendo il rispetto dei diritti fondamentali.

L'esempio di ChatGPT trova un parziale riscontro nell'AI Act, che stabilisce in via introduttiva che *“per taluni sistemi specifici di IA, vengono proposti soltanto obblighi minimi di trasparenza, in particolare quando vengono utilizzati chatbot o deep fake”*.

Trattasi del resto di una tecnologia in fase di sviluppo; sebbene il chatbot in questione sia in grado di fornire informazioni su qualsiasi argomento, esso non potrebbe in alcun modo comportare rischi nei settori precedentemente menzionati, né rimpiazzare l'uomo, a causa delle limitazioni nelle risposte del software.

Sono viceversa proposte previsioni più incisive volte ad affrontare i problemi scaturenti dai sistemi di IA *“ad alto rischio”*, ritenuti in grado di produrre effetti sui diritti fondamentali, nonché la salute e la sicurezza. Basandosi su un *“approccio proporzionato basato sul rischio”*, la proposta stabilisce misure e regole applicate dagli Stati membri a mezzo di un sistema di governance basato su strutture esistenti volto a gestire efficacemente i pericoli dei sistemi sopraccitati.

Le misure in questione riguardano sistemi di IA utilizzabili per mettere in atto pratiche ritenute particolarmente dannose e dunque da vietare, di cui si tratterà approfonditamente.

## 4.2 La struttura generale della proposta

Prima di fornire una panoramica dei titoli in cui è suddiviso il regolamento proposto, occorre esaminare in via preliminare la base giuridica e i relativi criteri.

Essa definisce il proprio obiettivo principale come il “*buon funzionamento del mercato interno fissando regole armonizzate*”, specie con riguardo allo “*sviluppo, l'immissione sul mercato dell'Unione e l'utilizzo di prodotti e servizi che ricorrono a tecnologie di intelligenza artificiale o forniti come sistemi di IA indipendenti ('stand-alone')*”<sup>179</sup>.

Il fondamento normativo della proposta è costituito dall'art. 114 TFUE<sup>180</sup>, nella parte in cui prevede l'adozione di misure volte assicurare l'instaurazione ed il funzionamento del mercato interno.

### **Trattato sul funzionamento dell'Unione europea – Articolo 114:**

*1. Salvo che i trattati non dispongano diversamente, si applicano le disposizioni seguenti per la realizzazione degli obiettivi dell'articolo 26. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria e previa consultazione del Comitato economico e sociale, adottano le misure relative al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno.*

Avendo come obiettivo l'armonizzazione dei sistemi giuridici degli Stati membri, la proposta stabilisce standard obbligatori nell'ambito della progettazione e lo sviluppo dei sistemi IA, specie con riguardo a quelli di maggiore impatto sui settori previamente citati.

---

<sup>179</sup> AI Act, p. 6.

<sup>180</sup> Versione consolidata del trattato sul funzionamento dell'Unione europea, Capo 3: Ravvicinamento delle legislazioni - Articolo 114.1 (ex articolo 95 del TCE), <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:12008E114&from=EL>

Occorre rilevare come la proposta stabilisca regole direttamente concernenti la protezione delle persone fisiche nell'ambito del trattamento dei dati personali basate sull'art. 16 TFUE<sup>181</sup>.

**Trattato sul funzionamento dell'Unione europea – Articolo 16:**

1. *Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.*
2. *Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti.*

[...]

La normativa sopraccitata è alla base delle restrizioni e tutele previste con riguardo ai sistemi di IA che comportano rischi con un considerevole impatto, quali quelli utilizzati per la "identificazione biometrica remota 'in tempo reale' in spazi accessibili al pubblico a fini di attività di contrasto", di cui si tratterà approfonditamente.

I titoli in cui è suddivisa la proposta di regolamento, il cui scopo è l'applicazione omogenea di nuove regole concernenti i sistemi di IA, rispondono a criteri di sussidiarietà e proporzionalità<sup>182</sup>.

---

<sup>181</sup> Versione consolidata del trattato sul funzionamento dell'Unione europea, Capo 3: Ravvicinamento delle legislazioni - Articolo 16.1 e 16.2 (ex articolo 286 del TCE), <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:12008E114&from=EL>

<sup>182</sup> AI Act, p. 7.

Per quanto concerne il criterio di sussidiarietà, la proposta suggerisce che gli obiettivi della stessa non possano essere raggiunti efficacemente dai singoli stati membri. Onde evitare una eccessiva frammentazione delle regole applicate nell'ambito dell'intelligenza artificiale e la creazione di normative contraddittorie che possano potenzialmente ostacolare il corretto funzionamento del mercato interno nelle ipotesi in cui sia utilizzata l'IA, il regolamento può fornire un quadro giuridico omogeneo in grado di far fronte alle esigenze sinora approfondite, al di fuori delle fattispecie rientranti nella competenza esclusiva.

La proposta, come precedentemente menzionato, segue un approccio basato sul rischio comportato dall'uso di determinati sistemi di IA. Al fine di far fronte ai rischi concernenti i diritti fondamentali e la sicurezza, il regolamento proposto segue un criterio di proporzionalità, intervenendo sui requisiti delle tecnologie in esame in modo più o meno incisivo.

Gli oneri normativi previsti comportano “*requisiti di qualità elevata dei dati, documentazione e tracciabilità, trasparenza, sorveglianza umana, precisione e robustezza*” nelle ipotesi dei sistemi di IA ad alto rischio; questi saranno viceversa attenuati qualora siano utilizzati sistemi non appartenenti a tale categoria.

Segue una sintesi dei punti di maggiore rilievo per la presente trattazione della struttura generale della proposta, che delinea in via preliminare il contenuto dei titoli del regolamento nel capo concernente l'illustrazione delle singole disposizioni<sup>183</sup>. Le definizioni contenute nei titoli saranno esaminate approfonditamente nel corso della presente trattazione.

Il **Titolo I (Ambito di applicazione e definizioni)** riguarda l'ambito di applicazione e le definizioni. Esso individua l'oggetto del regolamento e l'ambito di applicazione delle regole concernenti l'utilizzo di sistemi di IA nel mercato interno; fornisce inoltre le definizioni utilizzate in tutto l'atto, svolgendo una funzione simile a quella dell'art. 4 del GDPR.

---

<sup>183</sup> AI Act, pp. 13-18.

Occorre anzitutto citare la definizione di sistema di IA fornita dall'art. 3 dell'AI Act<sup>184</sup>:

### **AI Act – Articolo 3: Definizioni**

*1) "sistema di intelligenza artificiale" (sistema di IA): un software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono;*

Il Considerando 3<sup>185</sup> reitera come la famiglia di tecnologie di cui è parte l'intelligenza artificiale sia in rapida evoluzione, e l'utilizzabilità di tali sistemi per ottenere numerosi benefici dal punto di vista socioeconomico, nonché per lo svolgimento di attività industriali.

Rileva con riguardo al Titolo I anche il Considerando 1<sup>186</sup>, che reitera come l'uso dell'intelligenza artificiale debba conformarsi ai valori dell'Unione. Esso elenca una serie di motivi di interesse pubblico, quali:

- Un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali;
- La libera circolazione transfrontaliera di beni e servizi basati sull'IA,
- Impedire restrizioni eccessive allo sviluppo, alla commercializzazione e all'uso di sistemi di IA.

Il **Titolo II** definisce ed elenca le pratiche di intelligenza artificiale vietate secondo i criteri dell'approccio basato sul rischio, che saranno trattate approfonditamente nel corso della presente trattazione.

---

<sup>184</sup> AI Act, art. 3, comma I.

<sup>185</sup> AI Act, Considerando 3.

<sup>186</sup> AI Act, Considerando 1.

Il regolamento suddivide i sistemi di IA in una piramide di criticità a tre livelli, a seconda che l'uso di questi crei:

1. *Un rischio inaccettabile;*
2. *Un rischio alto (sistemi di IA ad alto rischio);*
3. *Un rischio basso o minimo.*

Il **Titolo III** concerne il secondo livello della piramide di criticità precedentemente delineata, ossia i “*sistemi di IA ad alto rischio*”. La proposta prevede la possibilità di immettere questi nel mercato europeo nel rispetto di determinati requisiti e in seguito a valutazioni della conformità allo scopo di tutelare le persone fisiche, potendo tali sistemi incidere sulla loro salute, sicurezza e diritti fondamentali. La proposta stabilisce le regole di classificazione dei sistemi in base alla funzione da essi svolta, nonché le modalità del relativo funzionamento.

Il **titolo IV (Obblighi di trasparenza per determinati sistemi di IA)** concerne i rischi di manipolazione comportati da taluni sistemi di IA, cui è necessario applicare specifici obblighi di trasparenza e di informazione, facendo sì che le persone siano informate dell'utilizzo di mezzi automatizzati in determinati contesti, onde tutelarne la facoltà di compiere scelte informate. La proposta elenca le seguenti ipotesi:

1. *Sistemi che interagiscono con gli esseri umani;*
2. *Sistemi utilizzati per:*
  - a. *Rilevare emozioni;*
  - b. *Stabilire un'associazione con categorie sociali sulla base di dati biometrici;*
3. *Sistemi che generano o manipolano contenuti a mezzo di tecnologie “deep fake”.*

Occorre menzionare anche i **Titolo VI (Governance)** e **VII (Banca dati dell'UE per i sistemi di IA indipendenti ad alto rischio)**. Il primo istituisce il comitato europeo per l'intelligenza artificiale, onde attuare efficacemente e in modo armonizzato il quadro giuridico delineato dal regolamento, favorendo in tal modo la cooperazione tra le autorità di controllo degli Stati membri e la Commissione, ad esempio condividendo le migliori pratiche da esso raccolte.

In particolare, gli Stati membri sono tenuti a istituire un'autorità nazionale di controllo con funzioni simili a quelle del Garante per la protezione dei dati personali con riguardo all'attuazione del GDPR, in quanto ricopre il medesimo ruolo nei confronti dell'applicazione dell'AI Act. Il secondo prevede l'istituzione di una banca dati a livello dell'UE gestita dalla Commissione, onde facilitare il monitoraggio dei sistemi di IA ad alto rischio indipendenti in grado di incidere sui diritti fondamentali delle persone. L'efficacia della banca dati consiste nell'obbligo dei fornitori di registrare i sistemi di IA che intendano immettere sul mercato o mettere in servizio.

#### 4.3 Le metodologie di armonizzazione della proposta con la normativa UE esistente

La proposta in esame comporta necessariamente la necessità di assicurarne la coerenza con il diritto europeo vigente in materia di intelligenza artificiale. È anzitutto garantito il rispetto della Carta dei diritti fondamentali dell'Unione europea, nonché della normativa concernente la protezione dei dati per quanto riguarda settori ove sono già utilizzati o saranno utilizzabili nel futuro i sistemi di IA ad alto rischio. Ai fini della presente trattazione rileva osservare come la proposta non pregiudichi il GDPR, integrandolo con *“regole armonizzate applicabili alla progettazione, allo sviluppo e all'utilizzo di determinati sistemi di IA ad alto rischio”* e *“restrizioni concernenti determinati usi dei sistemi di identificazione biometrica remota”*.

Come precedentemente osservato, gli algoritmi di IA sono suscettibili di *bias* cognitivi; in ragione di ciò, la proposta integra il diritto UE in maniera tale da ridurre al minimo i rischi di discriminazione algoritmica con obblighi relativi al ciclo di vita dei sistemi di IA concernenti:

- Prove;
- Gestione dei rischi;
- Documentazione;
- Sorveglianza umana.



La proposta sarà inoltre coerente e complementare con ulteriori iniziative della Commissione concernenti il settore dell'intelligenza artificiale, che potranno dunque integrarla a scopo di chiarezza giuridica. In particolare, ne è garantita la coerenza con quanto la Commissione ha annunciato per quanto riguarda il proprio obiettivo di contribuire alla *“promozione della tecnologia al servizio delle persone”*.

In particolare, essa ha delineato tre obiettivi principali:

- *Una tecnologia al servizio delle persone: sviluppare, diffondere e adottare tecnologie che migliorino sensibilmente la vita quotidiana delle persone. Un'economia forte e competitiva che domini e plasmi la tecnologia nel rispetto dei valori europei.*
- *Un'economia equa e competitiva: un mercato unico senza attriti, in cui le imprese di tutte le dimensioni e in qualsiasi settore possano competere in condizioni di parità e possano sviluppare, commercializzare e utilizzare tecnologie, prodotti e servizi digitali su una scala tale da rafforzare la loro produttività e la loro competitività a livello mondiale, e in cui i consumatori possano essere certi che i loro diritti vengano rispettati.*
- *Una società aperta, democratica e sostenibile: un ambiente affidabile in cui i cittadini siano autonomi e responsabili nel modo in cui agiscono e interagiscono, anche in relazione ai dati che forniscono sia online sia offline. Un approccio europeo alla trasformazione digitale che rinforzi i nostri valori democratici, rispetti i diritti fondamentali e contribuisca a un'economia sostenibile, a impatto climatico zero ed efficiente nell'impiego delle risorse.*<sup>187</sup>

La promozione dell'innovazione così delineata è legata anche all'Atto sulla governance dei dati, che si propone di affrontare la questione del *“consenso all'utilizzo di dati personali con l'aiuto di un "intermediario per la condivisione dei dati personali”*, il cui compito consiste

---

<sup>187</sup> Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni - Plasmare il futuro digitale dell'Europa*, COM(2020) 67 final, 19 febbraio 2020, <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52020DC0067&from=IT>

*nell'aiutare i singoli individui a esercitare i propri diritti a norma del regolamento generale sulla protezione dei dati”, nonché il “consenso all'utilizzo dei dati per scopi altruistici”.*<sup>188</sup>

La proposta rafforza inoltre in maniera significativa il ruolo dell'Unione per quanto riguarda il contributo alla definizione di norme e standard globali e la promozione di un'IA affidabile che sia coerente con i valori e gli interessi dell'Unione.<sup>189</sup>

#### 4.4 Le pratiche di AI vietate

Il sopraccitato titolo II concerne i sistemi di IA che comportano un rischio inaccettabile: questi sono soggetti ai divieti più incisivi, in quanto mettono in atto pratiche contrarie ai valori dell'Unione, spesso comportanti violazioni di diritti fondamentali. La norma di riferimento è l'art. 5 dell'AI Act, che elenca numerose fattispecie. Essa vieta a priori l'“*immissione sul mercato, la messa in servizio o l'uso*” delle seguenti pratiche:

- Sistemi di intelligenza artificiale che utilizzano tecniche subliminali, non evidenti agli utilizzatori, per influenzare in maniera sostanziale il comportamento delle persone in una maniera tale da causare danni fisici o psicologici alle persone stesse o ad altri (ossia i *dark pattern* previamente analizzati);
- Lo sfruttamento delle vulnerabilità di specifici gruppi vulnerabili, inducendoli a comportarsi in maniera tale da provocare a se stessi o ad altri danni psicologici o fisici (es. minori, persone con disabilità).
- L'attribuzione di un punteggio sociale basato sull'IA per finalità generali da parte di autorità pubbliche.
- Il ricorso a sistemi di identificazione biometrica remota in tempo reale in spazi accessibili al pubblico a fini di attività di contrasto, salve determinate eccezioni quali esigenze di sicurezza.<sup>190</sup>

---

<sup>188</sup> Commissione europea, *Proposta di regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati (Atto sulla governance dei dati)*, 25 novembre 2020, <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52020PC0767>

<sup>189</sup> AI Act, p. 6.

<sup>190</sup> AI Act, art. 5.

Occorre anzitutto definire alcune espressioni che il regolamento utilizza frequentemente in tali contesti. Anzitutto, la *“immissione sul mercato”* consiste nella *“prima messa a disposizione di un sistema di IA sul mercato dell’Unione”*.

La *“messa a disposizione sul mercato”* concerne *“qualsiasi fornitura di un sistema di IA per la distribuzione o l’uso sul mercato dell’Unione nel corso di un’attività commerciale, a titolo oneroso o gratuito”*.

La *“messa in servizio”* è *“la fornitura di un sistema di IA direttamente all’utente per il primo uso o per uso proprio sul mercato dell’Unione per la finalità prevista”*.<sup>191</sup>

I sistemi di identificazione biometrica remota *“in tempo reale”* sono definiti come sistemi volti alla *“biometrica remota in cui il rilevamento dei dati biometrici, il confronto e l’identificazione avvengono senza ritardi significativi. Sono incluse non solo le identificazioni istantanee, ma anche quelle che avvengono con brevi ritardi limitati al fine di evitare l’elusione della normativa”*. L’identificazione può avvenire anche *“a posteriori”*, ossia in tutte le ipotesi che non rientrano nella fattispecie così delineata.

I dati biometrici in questione sono a loro volta definiti come i dati personali ottenuti da un *“trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l’identificazione univoca, quali l’immagine facciale o i dati dattiloscopici”*.

Infine, è qualificato come *“spazio accessibili al pubblico”* qualsiasi *“luogo fisico accessibile al pubblico, indipendentemente dall’applicabilità di determinate condizioni di accesso”*.

---

<sup>191</sup> AI Act, art 3, comma I.

Occorre rilevare come il Considerando 7<sup>192</sup> preveda che la nozione di dati biometrici sopraccitata debba essere in linea con quella contenuta nel GDPR; la questione sarà approfondita nel contesto dei punti di contatto fra esso e l'AI Act.

Il Considerando 8 offre ulteriori spunti concernenti i sistemi di identificazione biometrica remota dal punto di vista funzionale, stabilendo che essi effettuino l'identificazione in questione tramite il confronto dei dati biometrici di una persona con quelli contenuti in una banca dati di riferimento, senza sapere anticipatamente qualora vi sia un effettivo riscontro. Esso fornisce inoltre specificazioni per quanto concerne i sistemi di identificazione "in tempo reale", stabilendo come questi facciano uso di "*materiale "dal vivo" o "quasi dal vivo" generato da una telecamera o da altro dispositivo con funzionalità analoghe*".

Viceversa, i sistemi di identificazione "a posteriori" concernono dati biometrici già rilevati, e fanno uso di "*immagini o filmati generati da telecamere a circuito chiuso o da dispositivi privati*"; conseguentemente l'identificazione avviene in un secondo momento e non istantaneamente, trattandosi di materiale creato prima dell'uso del sistema.<sup>193</sup>

Il Considerando 23 reitera quanto stabilito in relazione all'art. 16 TFUE: le regole del regolamento proposto vietano l'uso di sistemi per l'identificazione biometrica remota "in tempo reale" di persone fisiche in spazi accessibili al pubblico a fini di attività di contrasto.

Esso, inoltre, specifica come le norme contenute nell'AI Act debbano applicarsi come *lex specialis* rispetto alle regole concernenti il trattamento dei dati biometrici contenuti nell'art. 10 della direttiva 2016/680, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.<sup>194</sup>

---

<sup>192</sup> AI Act, Considerando 7.

<sup>193</sup> AI Act, Considerando 8.

<sup>194</sup> AI Act, Considerando 23.

L'AI Act, dunque, si applica ai “*dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, e il trattamento di dati genetici, di dati biometrici intesi a identificare in modo univoco una persona fisica o di dati relativi alla salute o di dati relativi alla vita sessuale della persona fisica o all'orientamento sessuale*”, prescindendo dall'autorizzazione dal diritto UE o dallo Stato membro o la salvaguardia di un interesse vitale della persona fisica.<sup>195</sup>

Il regolamento fornisce ulteriori dettagli per quanto concerne i sistemi di IA in grado di “*distorcere il comportamento umano e che possono provocare danni fisici o psicologici*”, specificamente un danno materiale a se stessa o ad altra. Il comportamento è distorto a mezzo di azioni che impiegano componenti subliminali, o agiscono su soggetti particolarmente vulnerabili, salvo il comportamento non dipenda da fattori esterni al sistema di IA.<sup>196</sup>

Il Considerando 17 elabora il concetto di punteggio sociale menzionato nell'art. 5. Esso è finalizzato alla valutazione della “*affidabilità delle persone fisiche*” sulla base di fattori quali:

- Il comportamento sociale;
- Caratteristiche personali;
- Caratteristiche della personalità note o previste.

Il punteggio in questione è attribuito a mezzo di sistemi IA da autorità pubbliche alle persone fisiche, portando potenzialmente a discriminazioni a mezzo di trattamenti pregiudizievoli o sfavorevoli, nonché lesioni della dignità.<sup>197</sup>

---

<sup>195</sup> Gazzetta ufficiale dell'Unione europea, *Direttiva (UE) 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione*, <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L0680&from=RO#:~:text=La%20tecnologia%2C%20come%20mai%20in,l'esecuzione%20di%20sanzioni%20penali.>

<sup>196</sup> AI Act, Considerando 16.

<sup>197</sup> AI Act, Considerando 17.

Un esempio di sistema basato sul punteggio sociale è fornito dal *social credit system* sperimentato dal governo cinese. La componente tecnologica del sistema in questione consente un monitoraggio diretto e diffuso, fondato su molteplici canali automatizzati di approvvigionamento dei dati con finalità di profilazione. Esso consente di creare e gestire dati e di condividere tali informazioni con le autorità coinvolte.

Il punteggio determinato dal sistema è “accreditato” in tempo reale, e permette agli uffici coinvolti di visualizzarlo, per poi determinare a quali servizi abbia diritto il cittadino o l’azienda.<sup>198</sup>

#### 4.5 I divieti d’uso dell’AI: la valutazione dei sistemi ad ‘alto rischio’

I sistemi di Intelligenza Artificiale ad alto rischio sono soggetti a un regime di certificazione dettagliato, ma non sono ritenuti pericolosi al punto da dover essere vietati.

Il **capo 1 del titolo III** individua anzitutto due categorie al cui interno rientrano sistemi di IA ad alto rischio comportanti rischi già concretizzatisi, o che potranno sorgere nel prossimo futuro.

- 1. I sistemi di IA destinati ad essere utilizzati come componenti di sicurezza di prodotti soggetti a valutazione della conformità ex ante da parte di terzi;*
- 2. Altri sistemi di IA indipendenti che presentano implicazioni principalmente in relazione ai diritti fondamentali esplicitamente elencati nell'allegato III.*

L’allegato III citato nella norma riportata è di fondamentale rilevanza, poiché i sistemi in esso indicati dovranno soddisfare la maggior parte dei requisiti del regolamento.

---

<sup>198</sup> Agenda Digitale, Berti R., *Il Social Credit System cinese: un esempio di big data al servizio del potere*, 30 aprile 2019, <https://www.agendadigitale.eu/cultura-digitale/il-social-credit-system-cinese-un-esempio-di-big-data-al-servizio-del-potere/>

Esso concerne i sistemi di IA ad alto rischio cui rimanda l'art. 6 del regolamento sull'IA, includendovi, a titolo esemplificativo, i già citati “*sistemi di IA destinati a essere utilizzati per l'identificazione biometrica remota ‘in tempo reale’ e ‘a posteriori’ delle persone fisiche*”.

Esso include anche sistemi concernenti la gestione e il funzionamento delle infrastrutture critiche, l'istruzione e la formazione professionale, nonché l'occupazione, la gestione dei lavoratori e l'accesso al lavoro autonomo.<sup>199</sup>

Il **capo 2 del titolo III** concerne i requisiti giuridici per i sistemi di IA ad alto rischio, in relazione a:

- Dati;
- Governance dei dati;
- Documentazione delle registrazioni;
- Conservazione delle registrazioni;
- Trasparenza;
- Fornitura di informazioni agli utenti;
- Sorveglianza umana;
- Robustezza;
- Accuratezza;
- Sicurezza.

La proposta specifica come i requisiti riportati garantiscano la compatibilità del quadro normativo del regolamento sull'IA con gli standard adottati dai partner commerciali dell'Unione, in quanto tengono in considerazione le raccomandazioni e i principi internazionali del settore.

---

<sup>199</sup> Commissione Europea, *Allegati della proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, Bruxelles, Allegato III, 21 aprile 2021, , p. 4; [https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0006.02/DOC\\_2&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0006.02/DOC_2&format=PDF)

Il **capo 3 del titolo III** riguarda obblighi proporzionati per i fornitori di sistemi di IA, gli utenti ed altre figure potenzialmente rilevanti nel settore dell'IA quali importatori, distributori e rappresentanti autorizzati.

Seguono i **capi 4 e 5 del titolo III**, concernenti le procedure di valutazione della conformità per ciascun tipo di sistema di IA ad alto rischio, che saranno trattate approfonditamente nei paragrafi successivi. Esse hanno lo scopo di minimizzare l'onere in capo agli operatori economici e per gli organismi in questione; i capi definiscono il quadro normativo per gli *“organismi notificati che saranno coinvolti come terze parti indipendenti”*. L'allegato III menziona inoltre sistemi di IA ad alto rischio c.d. indipendenti, per i quali è prevista l'istituzione di un nuovo sistema di conformità. Rileva l'art. 6 del regolamento proposto, concernente le relative regole di classificazione:

#### **AI Act – Articolo 6: Regole di classificazione per i sistemi di IA ad alto rischio**

*1. A prescindere dal fatto che sia immesso sul mercato o messo in servizio in modo indipendente rispetto ai prodotti di cui alle lettere a) e b), un sistema di IA è considerato ad alto rischio se sono soddisfatte entrambe le condizioni seguenti:*

*a) il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato II;*

*b) il prodotto, il cui componente di sicurezza è il sistema di IA, o il sistema di IA stesso in quanto prodotto è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato II.*

*2. Oltre ai sistemi di IA ad alto rischio di cui al paragrafo 1, sono considerati ad alto rischio anche i sistemi di IA di cui all'allegato III.<sup>200</sup>*

---

<sup>200</sup> AI Act, art. 6.



La proposta menziona come già nel 2020 il Consiglio europeo abbia invitato a definire in dettaglio quali sistemi debbano essere considerate ad alto rischio.<sup>201</sup> Come si è detto, l'AI Act prevede metodologie di gestione del rischio concernenti i sistemi di IA che pongono “rischi significativi per la salute e la sicurezza o per i diritti fondamentali delle persone”, nonché obblighi “prevedibili, proporzionati e chiari” in capo ai fornitori degli stessi <sup>202</sup>.

Occorre citare la nozione di “fornitore” contenuta nella proposta, che definisce tale figura come segue:

### **AI Act – Articolo 3: Definizioni**

[...]

2) "fornitore": una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o che fa sviluppare un sistema di IA al fine di immetterlo sul mercato o metterlo in servizio con il proprio nome o marchio, a titolo oneroso o gratuito;

[...]

Con riguardo al criterio di proporzionalità precedentemente esaminato, al fine di tutelare efficacemente i diritti fondamentali e la sicurezza delle persone fisiche, la proposta prevede la necessità di requisiti di “qualità elevata dei dati, documentazione e tracciabilità, trasparenza, sorveglianza umana, precisione e robustezza”.<sup>203</sup>

Al fine di monitorare efficacemente l'uso dei sistemi di IA ad alto rischio, la proposta prevede che la Commissione svolga tale funzione a mezzo di un “sistema di registrazione delle applicazioni di IA ad alto rischio indipendenti in una banca dati pubblica a livello dell'UE”, cui i sopraccitati fornitori di IA dovranno comunicare le informazioni concernenti

<sup>201</sup> Consiglio europeo, Riunione speciale del Consiglio europeo (1° e 2 ottobre 2020) – Conclusioni EUCO 13/20, 2020, <https://www.consilium.europa.eu/media/45923/021020-euco-final-conclusions-it.pdf>

<sup>202</sup> AI Act, p. 3.

<sup>203</sup> AI Act, p. 7.

i sistemi e le relative valutazioni della conformità. Il Considerando 32 definisce i sistemi indipendenti in questione come *“sistemi IA ad alto rischio diversi da quelli che sono componenti di sicurezza di prodotti o che sono essi stessi prodotti”*.<sup>204</sup>

A mezzo della banca dati, le autorità competenti e gli utenti avranno la possibilità di verificare qualora il sistema di IA ad alto rischio rispetti effettivamente i requisiti obbligatori previsti dal regolamento.<sup>205</sup>

Rileva in tal senso anche l’art. 14 del regolamento, ai sensi del quale i sistemi di IA ad alto rischio sono sviluppati in modo tale da poter essere *“efficacemente supervisionati da persone fisiche durante il periodo in cui il sistema di IA è in uso”* onde affrontare i rischi per la salute, la sicurezza o i diritti fondamentali.<sup>206</sup>

La proposta specifica inoltre come determinati sistemi di IA rientrino nell’ambito dell’AI Act anche qualora non siano immessi sul mercato, né messi in servizio, né utilizzati nell’Unione, menzionando a titolo esemplificativo la circostanza in cui *“un operatore stabilito nell’Unione che [appalti] alcuni servizi a un operatore stabilito al di fuori dell’Unione in relazione a un’attività che deve essere svolta da un sistema di IA che sarebbe classificato ad alto rischio e i cui effetti avrebbero un impatto sulle persone fisiche che si trovano nell’Unione”*.

Onde evitare che l’operatore al di fuori dell’Unione eluda quanto previsto dal regolamento, questo deve applicarsi anche a fornitori ed utenti in un paese terzo, *“nella misura in cui l’output prodotto da tali sistemi è utilizzato nell’Unione”*.

---

<sup>204</sup> AI Act, Considerando 32.

<sup>205</sup> AI Act, p. 13.

<sup>206</sup> AI Act, art. 14.

Ciò non vale nelle ipotesi di cooperazione con partner stranieri per lo scambio di informazioni ed elementi probatori; in tali casi il regime sopra delineato non si applicherà alle autorità pubbliche del paese terzo in questione e alle organizzazioni internazionali nell'ambito della cooperazione delle autorità giudiziarie e di contrasto con l'Unione o con i suoi Stati membri.<sup>207</sup>

Ai sensi dell'art. 43 e del relativo capo, la verifica del rispetto dei requisiti dei sistemi di IA ad alto rischio deve avvenire secondo “procedure di valutazione della conformità”, ossia tramite modalità simili a quelle già adottate per altri prodotti regolamentati a livello europeo. In taluni casi il fornitore valuta in maniera autonoma la conformità dei propri sistemi di IA ai requisiti del Regolamento, mentre per altri sistemi sarà necessario coinvolgere un organismo esterno.<sup>208</sup>

Compete agli organismi notificati ex art. 33 la verifica della conformità del sistema di IA ad alto rischio secondo le procedure di valutazione sopraccitate; definiti come “*organismi di valutazione della conformità designati in conformità al presente regolamento e ad altre pertinenti normative di armonizzazione dell'Unione*”<sup>209</sup>, essi devono soddisfare i requisiti organizzativi, di gestione della qualità e relativi alle risorse e ai processi necessari all'assolvimento dei loro compiti.<sup>210</sup>

Rileva anche l'art. 48, ai sensi del quale il fornitore compila una dichiarazione scritta di conformità identificativa del sistema di IA per il quale è stata redatta, la quale è messa a disposizione delle autorità nazionali competenti.<sup>211</sup>

---

<sup>207</sup> AI Act, Considerando 11.

<sup>208</sup> AI Act, art. 43.

<sup>209</sup> AI Act, art. 3, comma I, n. 22.

<sup>210</sup> AI Act, art. 33.

<sup>211</sup> AI Act, art. 48.

## 4.6 Le responsabilità

Come si è detto in relazione ai motivi e obiettivi della proposta, essa mira ad evitare una frammentazione del mercato interno su elementi quali la responsabilità.

Il Parlamento europeo ha adottato già nel 2020 risoluzioni concernenti l'IA, alcune di queste riguardanti raccomandazioni alla Commissione sulla necessità di un regime di responsabilità civile adatto al settore.

In particolare, il Parlamento ha stabilito come, sebbene non ritenesse necessaria una sostanziale revisione dei regimi di responsabilità correttamente funzionanti, la *“complessità, la connettività, l'opacità, la vulnerabilità, la capacità di modifica mediante aggiornamenti, l'autoapprendimento e la potenziale autonomia dei sistemi di IA, come pure la molteplicità degli attori coinvolti nel settore”* avrebbero comportato la necessità di adeguamenti regimi di responsabilità, onde evitare che le persone non ottengano un risarcimento qualora subiscano un pregiudizio o danni al patrimonio.<sup>212</sup>

La proposta prevede che il fornitore, in qualità di persona fisica o giuridica, si assuma la responsabilità di immissione sul mercato o della messa in servizio dei sistemi di IA ad alto rischio, prescindendo dall'ipotesi in cui questi abbia progettato o meno il sistema. Ciò non vale per i sistemi di identificazione biometrica remota di persone, nella misura in cui questi non siano vietati: in tali casi è necessaria la valutazione di conformità di un organismo notificato. Sono inoltre stabilite responsabilità specifiche per gli utenti dei sistemi in questione al fine di garantire il monitoraggio delle relative prestazioni, onde tutelare la sicurezza e i diritti fondamentali.<sup>213</sup>

---

<sup>212</sup> Parlamento europeo, *Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale*, [https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276\\_IT.html](https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_IT.html)

<sup>213</sup> AI Act, comb. disp. dei consideranda 53, 58, 64.

La dichiarazione scritta di conformità redatta dal fornitore fa inoltre sì che questi si assuma la responsabilità della conformità del sistema di IA ai requisiti previsti dalla proposta.<sup>214</sup>

Il regolamento stabilisce sensi del quale i fornitori di sistemi di IA ad alto rischio sono tenuti ad istituire un “*sistema di gestione della qualità che garantisce le conformità al presente regolamento*”. In particolare, questo deve comprendere “*un quadro di responsabilità che definisca le responsabilità della dirigenza e di altro personale*”.<sup>215</sup>

L’AI Act prevede anche norme concernenti la responsabilità degli organismi notificati. L’assegnazione delle relative responsabilità deve “*garantire la fiducia nelle prestazioni degli organismi notificati e nei risultati delle attività di valutazione della conformità che essi effettuano*”. Essi sottoscrivono un’assicurazione di responsabilità per le attività di valutazione in questione, salvo lo Stato membro non assuma a sua volta direttamente la responsabilità a norma del diritto interno o a causa di una propria azione.<sup>216</sup>

Nell’ipotesi in cui gli organismi notificati subappaltino incarichi legati alla valutazione di conformità, questi garantiscono che il subappaltatore le affiliate soddisfino i requisiti sopraccitati, e conservando in ogni caso la relativa responsabilità.<sup>217</sup>

---

<sup>214</sup> AI Act, art. 48, comma IV.

<sup>215</sup> AI Act, art. 17.

<sup>216</sup> AI Act, art. 33, commi III, VIII e IX.

<sup>217</sup> AI Act, art. 34, commi I e II.

## 4.7 Le sanzioni

La proposta stabilisce in via preliminare come gli Stati membri debbano stabilire “*sanzioni effettive, proporzionate e dissuasive*” qualora le norme previste non siano rispettate; è inoltre prevista la possibilità per il Garante europeo della protezione dei dati di infliggere sanzioni pecuniarie ad istituzioni, agenzie e organismi UE rientranti nell’ambito del regolamento.<sup>218</sup>

Il titolo X della proposta prevede le sanzioni in questione, che devono soddisfare i tre requisiti sopraccitati, e stabilendo che gli Stati membri debbano stabilire le regole da applicare in caso di violazione del regolamento, garantendone in tal modo l’attuazione, nonché notificarle alla Commissione. Per determinare l’importo si tiene conto delle “*circostanze pertinenti*” e dei seguenti requisiti:

- a) la natura, la gravità e la durata della violazione e delle sue conseguenze;*
- b) se altre autorità di vigilanza del mercato hanno già applicato sanzioni amministrative pecuniarie allo stesso operatore per la stessa violazione;*
- c) le dimensioni e la quota di mercato dell'operatore che ha commesso la violazione.*

Per quanto concerne le sanzioni amministrative pecuniarie imposte a istituzioni, agenzie e organismi dell’Unione, il Garante europeo deve tenere conto dei seguenti requisiti:

- a) la natura, la gravità e la durata della violazione e delle sue conseguenze;*
- b) la cooperazione con il Garante europeo della protezione dei dati al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi, compreso il rispetto delle misure precedentemente disposte dal Garante europeo della protezione dei dati nei confronti dell'istituzione, dell'agenzia o dell'organismo dell'Unione in relazione allo stesso tema;*
- c) eventuali precedenti violazioni analoghe commesse dall'istituzione, dall'agenzia o dall'organismo dell'Unione.*

---

<sup>218</sup> AI Act, Considerando 84.

In base al quadro normativo così delineato, le autorità competenti individuate dagli Stati membri potranno comminare sanzioni amministrative fino a 30.000.000€ o 6% del fatturato annuo mondiale.

Sono inoltre previste anche sanzioni amministrative pecuniarie nell'ipotesi in cui siano fornite informazioni *“inesatte, incomplete o fuorvianti”* agli organismi notificati ed alle autorità nazionali competenti.<sup>219</sup>

#### 4.8 I punti di contatto con il GDPR

La proposta stabilisce espressamente come essa non pregiudichi il GDPR, in particolare integrandolo con *“una serie di regole armonizzate applicabili alla progettazione, allo sviluppo e all'utilizzo di determinati sistemi di IA ad alto rischio nonché di restrizioni concernenti determinati usi dei sistemi di identificazione biometrica remota”*.<sup>220</sup>

Se ne evince, dunque, la natura complementare rispetto al Regolamento 2016/679, in particolare considerando la presenza di rinvii al GDPR all'interno della proposta stessa.

L'art. 22 del GDPR, concernente il processo decisionale automatizzato rappresenta il punto di contatto di maggiore rilevanza, poiché la norma concerne forme di trattamento quali la profilazione svolte a mezzo di tecnologie oggi inquadrabili come IA. Deve tuttavia essere osservato le garanzie fornite dalla norma in questione abbiano un ambito di applicazione limitato sotto alcuni profili, in quanto la norma si applica ai soli processi esclusivamente automatizzati.

---

<sup>219</sup> AI Act, artt. 71 e 72.

<sup>220</sup> AI Act, p. 4.

Affinché le tutele in questione siano applicabili, inoltre, il processo decisionale automatizzato deve produrre effetti giuridici che lo riguardano o incidere in modo analogo significativamente sulla sua persona.

Un punto di contatto esplicito è rintracciabile nel Considerando 7, ai sensi del quale la nozione di dati biometrici precedentemente esaminata debba essere in linea con quella fornita dall'art. 4, punto 14) del GDPR.<sup>221</sup> Segue un confronto fra le definizioni rispettivamente fornite dai due regolamenti.

*GDPR: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.*<sup>222</sup>

*AI Act: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.*<sup>223</sup>

Il Considerando 24 della proposta opera un ulteriore riferimento, stabilendo che il trattamento di dati biometrici o altri dati personali utilizzati da sistemi di identificazione biometrica diversi da quelli “in tempo reale in spazi accessibili al pubblico a fini di attività di contrasto, debbano soddisfare, a seconda dei casi, tutti i requisiti derivanti dall'articolo 9, paragrafo 1 del GDPR. La norma in questione prevede il divieto di trattamento delle categorie speciali di dati, che saranno trattate approfonditamente nel capitolo V.

---

<sup>221</sup> AI Act, Considerando 7.

<sup>222</sup> Regolamento 2016/679, art. 4, n. 14.

<sup>223</sup> AI Act, art. 3, comma I, n. 33.



L'articolo 10 della proposta, il cui capo concerne i requisiti per i sistemi di IA ad alto rischio, opera un rinvio alla norma sopraccitata. Esso prevede che I sistemi di IA ad alto rischio che utilizzano *“tecniche che prevedono l'uso di dati per l'addestramento di modelli”* sono sviluppati sulla base di *“set di dati di addestramento, convalida e prova”* debbano rispettare specifici criteri di qualità. Prevede quindi in capo ai fornitori dei sistemi di IA in questione la possibilità di trattare le categorie di dati elencate nell'art. 9, comma I del GDPR, *“nella misura in cui ciò sia strettamente necessario al fine di garantire il monitoraggio, il rilevamento e la correzione delle distorsioni”*<sup>224</sup>.

È previsto un rinvio anche dall'art. 29 dell'AI Act, concernente gli obblighi degli utenti dei sistemi di IA ad alto rischio, a norma del quale questi usano le informazioni fornite a norma della proposta al fine di effettuare una valutazione obbligatoria d'impatto concernente la protezione dei dati ex art. 35 del regolamento (UE) 2016/679.

Tanto la proposta di Regolamento quanto il GDPR prescrivono infatti la valutazione del rischio di impatto sui diritti fondamentali e richiedono, conseguentemente, l'identificazione delle relative soluzioni di mitigazione, sebbene con alcune diversificazioni sostanziali.

Specificamente, il GDPR prevede nella Sezione 3 che trattamenti facenti uso di *“nuove tecnologie”* possono comportare rischi per i *“diritti e la libertà delle persone fisiche”*, tenendo conto di caratteristiche del trattamento quali *“la natura, l'oggetto, il contesto, le finalità”*.

---

<sup>224</sup> AI Act, art. 10, commi I e V.

Il Regolamento prevede che il titolare del trattamento compia una “*valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali*”, in particolare nei seguenti casi:

**Regolamento 2016/679 – Articolo 35:**

- a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;*
- b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o*
- c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.<sup>225</sup>*

Può evincersi come la norma in esame costituisca oggi un punto di contatto con la normativa prevista dall'AI Act, in ragione dei numerosi rischi derivanti dall'uso di determinati sistemi di intelligenza artificiale, quali i sistemi di identificazione biometrica remota in “tempo reale”.

L'AI Act ed il Regolamento (UE) 2016/679 presentano un ulteriore punto di contatto per quanto concerne il relativo ambito di applicazione. Entrambi prevedono anzitutto l'applicabilità delle rispettive regole indipendentemente dal fatto che gli operatori economici, quali i fornitori o i titolari o i responsabili del trattamento, siano stabiliti nell'UE.

Rileva in tal senso quanto stabilito nell'art. 2 della proposta. La norma, stabilisce espressamente l'applicabilità del regolamento ai “*fornitori che immettono sul mercato o mettono in servizio sistemi di IA nell'Unione, indipendentemente dal fatto che siano stabiliti nell'Unione o in un paese terzo*”, nonché ai relativi “*utenti*”.

---

<sup>225</sup> Regolamento 2016/679, art. 35.

Come precedentemente osservato nell'ambito della responsabilità, inoltre, Il regolamento si applica anche a fornitori situati in paesi terzi qualora l'output del relativo sistema sia *“utilizzato nell'Unione”*.<sup>226</sup>

Ai sensi del GDPR, la norma vigente è applicabile al trattamento dei dati personali effettuato dal titolare o dal responsabile nell'Unione, indipendentemente dalla circostanza che questo sul territorio di questa o meno. Se il titolare o il responsabile non si trova nell'Unione, analogamente alle ipotesi di *output* utilizzati nell'Unione, il Regolamento in esame è applicato nell'ipotesi in cui il trattamento concerna il monitoraggio o l'offerta di beni o servizi ad *“interessati che si trovano nell'Unione”*.

Specificamente, l'applicabilità del Regolamento in questione dipende dalla circostanza che il titolare o il responsabile abbiano uno stabilimento nell'Unione europea, nonché qualora il trattamento sia svolto nel contesto dell'attività dello stabilimento in questione. In tali ipotesi non rileverà il fatto che il trattamento abbia ad oggetto i dati personali di persone fisiche presenti nell'Unione europea ovvero in Paesi terzi.

In caso contrario occorrerà verificare qualora l'interessato si trovi all'interno dell'Unione, nonché se il trattamento avvenga nell'ambito di un'offerta di beni e servizi verso un Paese membro, ovvero di un'attività di monitoraggio degli interessati.<sup>227</sup>

Tenendo conto dell'attuale contesto globalizzato di commercializzazione di beni e servizi immateriali per i quali è estremamente difficile, se non impossibile, definire confini territoriali (ad esempio, i sistemi distribuiti cloud), è dunque evidente stabilire regole che riguardano non solo l'accesso al mercato dell'UE ma anche, più generalmente, l'accesso ai suoi consumatori e utenti.

---

<sup>226</sup> AI Act, art. 2, comma I.

<sup>227</sup> Riccio G. M., Scorza G., Belisario E., *GDPR e Normativa Privacy – Commentario*, Wolters Kluwer, 2022, p.22.

## CAPITOLO V

### Elaborazione dati e categorie speciali

#### 5.1 Trattamento di categorie particolari di dati personali

Il GDPR identifica le c.d. “*categorie particolari di dati personali*”, definiti anche come “*dati sensibili*” dal D.Lgs. 196/03 (Codice della Privacy). L’art. 9, concernente il “*trattamento di categorie particolari di dati personali*”, ne prevede il divieto di trattamento. Trattasi, dunque, di:

- Dati personali che rivelino:
  - L’origine razziale;
  - L’origine etnica;
  - Le opinioni politiche;
  - Le convinzioni religiose o filosofiche;
  - L’appartenenza sindacale;
- Dati genetici;
- Dati biometrici intesi a identificare in modo univoco una persona fisica;
- Dati relativi a:
  - Salute;
  - Vita sessuale;
  - Orientamento sessuale.

Il successivo comma elenca numerose ipotesi concernenti i motivi validi ai fini della liceità del trattamento dei categorie particolari di dati personali. Rileva anzitutto il consenso esplicito dell’interessato per finalità specifiche (salvo espresso divieto *ex lege* anche in presenza di esso), o il caso in cui i dati personali siano manifestamente resi pubblici dall’interessato.

Talvolta, inoltre, il trattamento di categorie speciali di dati può essere previsto come obbligo legale in capo al responsabile del trattamento in materia, ad esempio, di lavoro o sicurezza. Esso potrebbe anche essere necessario per l'istituzione, l'esercizio o la difesa in sede giudiziaria, nonché quando le autorità giurisdizionali agiscono nel loro ruolo.

Rilevano anche le esigenze di protezione degli interessi vitali dell'interessato o di un'altra persona, qualora la persona interessata sia legalmente o fisicamente incapace di dare il consenso, nonché attività legittime di un'organizzazione senza fini di lucro con un obiettivo politico, filosofico o sindacale.

La norma menziona anche le ipotesi di sostanziale interesse pubblico sulla base della normativa UE o nazionale, il quale deve essere proporzionato all'obiettivo perseguito, rispettando l'essenza del principio del diritto alla protezione dei dati e con la previsione di misure specifiche per difendere i diritti e le libertà fondamentali dell'interessato. Sono prese in considerazione anche esigenze di sanità pubblica, archiviazione nell'interesse pubblico, o scopi di ricerca e statistica.<sup>228</sup>

Occorre esaminare anche quanto disposto dall'art. 22 del GDPR in materia. Come precedentemente approfondito, esso stabilisce che *“l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona”*. La disposizione sopraccitata, ai sensi del paragrafo 2, non dovrebbe applicarsi nel caso in cui la decisione automatizzata:

- Sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
- Sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
- Si basi sul consenso esplicito dell'interessato.

---

<sup>228</sup> Regolamento 2016/679, art. 9, commi I e II.

L'art. 22 opera, tuttavia, un rinvio all'art. 9 nel comma IV<sup>229</sup>:

**Regolamento 2016/679 – Art. 22: Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione**

*4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, della libertà e dei legittimi interessi dell'interessato.*

Pertanto, la decisione basata unicamente sul trattamento automatizzato diviene possibile in due ipotesi.

1. L'interessato ha *“prestato il proprio consenso esplicito al trattamento di tali dati personali [ossia i dati definiti nell'art. 9] per una o più finalità specifiche”* (eccetto qualora il diritto dell'Unione o degli Stati membri disponga che l'interessato non possa revocare il divieto di trattamento delle categorie particolari di dati).
2. La circostanza in cui il trattamento in questione sia *“necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri”*, nel rispetto dei seguenti requisiti:
  - a. Deve essere proporzionato alla finalità perseguita;
  - b. Deve rispettare l'essenza del diritto alla protezione dei dati;
  - c. Deve prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.
3. Nelle ipotesi sopraccitate, non devono essere in vigore norme che proibiscano il trattamento automatizzato di dati particolari a tutela di diritti, libertà e interessi legittimi dell'interessato.

---

<sup>229</sup> Regolamento 2016/679, art. 22, commi I, II e IV.

## 5.2 Rapporto pubblico-privato

Per quanto concerne la liceità del trattamento per motivi di interesse pubblico, rileva l'art. 6 del GDPR:

### **Regolamento 2016/679 – Art. 6: Liceità del trattamento**

*1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:*

[...]

*e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;*

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

*a) dal diritto dell'Unione; o*

*b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento.*

Ai sensi del GDPR, dunque, le autorità pubbliche elaborano dati appartenenti alle categorie speciali sinora esaminate qualora il trattamento sia necessario per eseguire un compito di interesse pubblico, o sussista una previsione esplicita *ex lege*. In particolare, i motivi di interesse pubblico in questione che giustificano il trattamento di dati particolari devono essere previsti esplicitamente dal diritto UE o nazionale<sup>230</sup>, seguendo un approccio basato sul criterio della proporzionalità rispetto alla finalità perseguita e tutelando in ogni caso i diritti fondamentali e gli interessi della persona destinataria del trattamento.<sup>231</sup>

<sup>230</sup> Regolamento 2016/679, art. 6, comma III.

<sup>231</sup> Riccio G. M., Scorza G., Belisario E., *GDPR e Normativa Privacy – Commentario*, Wolters Kluwer, 2022, p. 126.

A titolo esemplificativo, l'art. 9 prevede alla lettera *i* del paragrafo 2 la possibilità di svolgere il trattamento ove sia necessario per motivi di “*interesse pubblico*” nel settore della sanità pubblica in ipotesi quali:

- La protezione da gravi minacce per la salute a carattere transfrontaliero;
- La garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria, dei medicinali e dei dispositivi medici;
- Sulla base del diritto UE o nazionale, se le norme prevedono misure adeguate a tutelare i diritti e le libertà dell'interessato, nonché il segreto professionale.<sup>232</sup>

Il trattamento e la comunicazione di dati sanitari ed amministrativi costituiscono un'attività necessaria per la diagnosi e la cura dei soggetti. I dati in questione sono correlati al fine di rilevare la presenza di patologie, nonché individuare eventuali rischi connessi; seguono le esigenze di rendicontazione delle prestazioni degli Enti, nonché di valenza epidemiologica e di valore economico.

Seguono le ipotesi di trattamento per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. In tali casi deve essere assicurata la conformità alle garanzie previste dall'art. 89 del GDPR, ai sensi del quale devono essere tutelati i diritti e le libertà dell'interessato a mezzo di misure tecniche e organizzative adeguate, le quali possono includere la pseudonimizzazione.<sup>233</sup> Anche in questo caso è previsto un criterio di proporzionalità rispetto alla finalità perseguita.<sup>234</sup>

---

<sup>232</sup> Regolamento 2016/679, art. 9, comma II, lett. i).

<sup>233</sup> Regolamento 2016/679, art. 89, comma I.

<sup>234</sup> Regolamento 2016/679, art. 9, comma II, lett. j).



In tali casi è possibile, ad esempio, il trattamento dei dati concernenti lo stato di salute, la vita sessuale e l'origine razziale ed etnica, anche in assenza del consenso degli interessati, nelle ipotesi in cui ciò si riveli indispensabile per il raggiungimento delle finalità della ricerca, per scopi di ricerca scientifica in campo medico, biomedico o epidemiologico, da parte di università, enti o istituti di ricerca e società scientifiche, ricercatori che operano nell'ambito di dette università, enti, istituti di ricerca e soci di dette società scientifiche e di tutti gli esercenti le professioni sanitarie e degli organismi sanitari.<sup>235</sup>

### 5.3 Rapporto privato-privato

Per quanto concerne l'elaborazione di dati particolari nei rapporti tra privati, rileva a titolo esemplificativo quanto disposto dall'art. 9 in materia di lavoro.

La norma in questione autorizza il trattamento nella misura in cui questo sia necessario per *“assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale”*; rilevano anche in questo caso le relative norme UE o nazionali, nonché quanto previsto dalla contrattazione collettiva, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato.<sup>236</sup>

Il GDPR individua, dunque, nella necessità per finalità lavorative una delle possibili eccezioni al divieto di trattamento di dati particolari. Esso deve essere *“indispensabile per le finalità individuate”*<sup>237</sup>, e il consenso deve essere raccolto dal datore di lavoro a mezzo di moduli che ne riportino le ragioni.

---

<sup>235</sup> Riccio G. M., Scorza G., Belisario E., *GDPR e Normativa Privacy – Commentario*, Wolters Kluwer, 2022, p. 133.

<sup>236</sup> Regolamento 2016/679, art. 9, comma I, lett. b).

<sup>237</sup> Garante per la protezione dei dati personali, doc. web n. 5800451 - *Autorizzazione generale n. 1/2016: Trattamento dei dati sensibili nei rapporti di lavoro*, 15 dicembre 2016, <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/5800451>.

Ai sensi dell'art. 4 dello Statuto dei Lavoratori, è anche possibile utilizzare strumenti di controllo (specificamente “*impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori*”<sup>238</sup>) per esigenze di natura organizzativa e produttiva, nonché di sicurezza e tutela del patrimonio aziendale.<sup>239</sup>

L'art. 9 prevede anche le ipotesi di trattamento di dati particolari svolto da “*fondazioni, associazioni o altri organismo senza scopo di lucro*”, elencando diversi requisiti:

- Deve essere effettuato nell'ambito delle rispettive “*legittime attività e con adeguate garanzie*”;
- Deve perseguire finalità politiche, filosofiche, religiose o sindacali;
- Deve riguardare unicamente:
  - Membri;
  - Ex membri;
  - Persone che hanno regolari contatti con uno degli enti sopraccitati;
- I dati personali non debbono essere comunicati all'esterno senza il consenso dell'interessato.<sup>240</sup>

Nel contesto dell'emergenza causata dalla pandemia da Covid-19, sono state avanzate anche nel settore privato richieste concernenti la raccolta di dati sanitari al fine di rilevare la presenza di sintomi da Coronavirus. Il GPDP ha rilevato in tal senso come tale incarico sia riservato a soggetti qualificati e predeterminati, condannando la raccolta di dati particolari con metodologie diverse da quelle previste dal Ministero della Salute<sup>241</sup>.

---

<sup>238</sup> L. 300/1970 (Statuto dei Lavoratori), *Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento*, art. 4, <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1970-05-20:300!vig=>.

<sup>239</sup> Riccio G. M., Scorza G., Belisario E., *GDPR e Normativa Privacy – Commentario*, Wolters Kluwer, 2022, p. 118.

<sup>240</sup> Regolamento 2016/679, art. 9, comma I, lett. d).

<sup>241</sup> Garante per la protezione dei dati personali, *Coronavirus: Garante Privacy, no a iniziative "fai da te" nella raccolta dei dati. Soggetti pubblici e privati devono attenersi alle indicazioni del Ministero della salute e delle istituzioni competenti*, Roma, 2 marzo 2020, <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9282117>.

Inoltre, a seguito dell'approvazione dei vaccini e l'inizio della campagna vaccinale, il Garante ha fornito indicazioni generali in ambito di vaccinazione nei luoghi di lavoro concernenti il trattamento dei dati personali. In particolare, ha specificato che le attività di trattamento dei dati relativi alle vaccinazioni necessarie per finalità di medicina preventiva di medicina del lavoro inerenti all'art. 9, comma II, lett. h) e 3) sono effettuabili esclusivamente da un professionista sanitario.<sup>242 243</sup>

---

<sup>242</sup> Garante per la protezione dei dati personali, *Provvedimento del 13 maggio 2021 - Documento di indirizzo "Vaccinazione nei luoghi di lavoro: indicazioni generali per il trattamento dei dati personali"*, <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9585300>.

<sup>243</sup> Riccio G. M., Scorza G., Belisario E., *GDPR e Normativa Privacy – Commentario*, Wolters Kluwer, 2022, pp. 120-121.

## **Considerazioni conclusive**

Sebbene il Regolamento 2016/679 abbia svolto un'efficace opera di armonizzazione della normativa concernente il trattamento dei dati personali ed abbia delineato, attraverso norme di portata generale, un quadro giuridico applicabile ai sistemi di intelligenza artificiale, esso non fornisce strumenti adeguati alla tutela dei diritti fondamentali delle persone fisiche a fronte dei traguardi raggiunti dalla tecnologia nel settore del *machine learning*.

La proposta di regolamento del 2021 affronta egregiamente la questione, specie a mezzo della previsione delle categorie di sistemi IA che comportano rischi inaccettabili, con l'evidente scopo di scongiurare il pericolo di sconfinare, ad esempio, in vere e proprie forme di sorveglianza orwelliane tramite sistemi di identificazione biometrica remota in tempo reale in spazi pubblici.

L'AI Act costituisce tuttavia un mero punto di partenza, e necessiterà nel futuro prossimo di ulteriori integrazioni, potendosi evincere dai numerosi sistemi all'avanguardia menzionati nel corso della trattazione come sia in atto una vera e propria rivoluzione tecnologica, destinata a produrre effetti particolarmente incisivi dal punto di vista socioeconomico e politico.

## **Bibliografia generale**

Benanti P., *Human in the Loop*, Mondadori, 2022.

Bolognini L., Pelino E., Bistolfi C., *Il regolamento privacy europeo – Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè Editore, 2016.

Bygrave, Lee A, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford Academic, New York, ed. 2020.

Cassano G., Colarocco V., Gallus G. B., Micozzi F. P., *Il processo di adeguamento al GDPR*, Giuffrè, 2022.

Commissione europea, *Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia* (COM(2020) 65 final), 19 febbraio 2020.

D'Acquisto G., *Intelligenza Artificiale – Elementi*, Giappichelli, 2021.

Fjeld, Jessica and Achten, Nele and Hilligoss, Hannah and Nagy, Adam and Srikumar, Madhulika, *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI*, Berkman Klein Center Research Publication No. 2020-1, 15 gennaio 2020.

Genus, & Stirling, A., *Collingridge and the dilemma of control: Towards responsible and accountable innovation*, *Research Policy.*, 47(1), 2018, pp. 61–69.

Giannantonio E., Losano M. G., Zeno-Zencovich V., *La tutela dei dati personali – Commentario alla l. 675/1996*, CEDAM, 1997.

Haenlein, & Kaplan, A., *A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence*. *California Management Review.*, 61(4), 2019 pp. 3, 8.

Kuner C., Cate H. F., Lynskey O., Millard C., Loideain N. N., Svantesson D. J. B., *Expanding the artificial intelligence-data protection debate*, *International Data Privacy Law*, Volume 8, Issue 4, novembre 2018, pp. 289–292.

Lindholm, A., Wahlström, N., Lindsten, F., & Schön, T., *Machine Learning: A First Course for Engineers and Scientists*, Cambridge University Press, 2022.

Mathur A., Acar G., Friedman J. M., Lucherini E., Mayer J., Chetty M., Narayanan A., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*. *Proc. ACM Hum. - Comput. Interact.* 3, CSCW, Article 81, novembre 2019.

McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (2006). *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, *AI Magazine*, 27(4), 31 agosto 1955.

Pizzetti F., *Intelligenza Artificiale, protezione dei dati personali e regolazione*, Giappichelli Editore, 2018.

Pizzetti F., *Privacy e Diritto europeo della protezione dei dati personali. Dalla Direttiva 95/46 al Nuovo Regolamento Europeo*, Giappichelli, 2016.

Riccio G. M., Scorza G., Belisario E., *GDPR e Normativa Privacy – Commentario*, Wolters Kluwer, 2022.

Turing A., “*Computing Machinery and Intelligence*,” *Mind*, LIX/236, 1950.

Warren S. e Brandeis L., *The Right to Privacy*, *Harvard Law Review* 193, 1890.

Wirth N., *Hello marketing, what can artificial intelligence help you with?*, International Journal of Market Research: the Journal of the Market Research Society, 60(5), 2018, pp. 435–438.

## Sitografia

Agenda Digitale, Amato S., *Big data: cosa sono, tipologie, esempi e sfide dell'economia del dato*, 18 maggio 2020, <https://www.agendadigitale.eu/cittadinanza-digitale/big-data-cosa-sono-tipologie-esempi-e-sfide-delleconomia-del-dato/>

Agenda Digitale, Anselmi N., Olivi G., *Machine learning, i problemi per la privacy (e le possibili soluzioni)*, 8 febbraio 2019, <https://www.agendadigitale.eu/cultura-digitale/machine-learning-i-problemi-per-la-privacy-e-le-possibili-soluzioni/>

Agenda Digitale, Berti R., *Il Social Credit System cinese: un esempio di big data al servizio del potere*, 30 aprile 2019, <https://www.agendadigitale.eu/cultura-digitale/il-social-credit-system-cinese-un-esempio-di-big-data-al-servizio-del-potere/>

Agenda Digitale, Giribaldi D., *Intelligenza artificiale, tutti i pregiudizi (bias) che la rendono pericolosa*, 26 febbraio 2019, <https://www.agendadigitale.eu/cultura-digitale/intelligenza-artificiale-tutti-i-pregiudizi-bias-che-la-rendono-pericolosa/>

Agenda Digitale, Nanni S., *Cina: le linee guida etiche per l'uso dell'intelligenza artificiale*, 28 ottobre 2021, <https://www.agendadigitale.eu/cultura-digitale/cina-le-linee-guida-etiche-per-luso-dellintelligenza-artificiale/>

Agenda Digitale, Nicotra M., *Intelligenza artificiale, cos'è, come funziona e le applicazioni in Italia ed Europa*, 23 maggio 2018, <https://www.agendadigitale.eu/sicurezza/privacy/intelligenza-artificiale-la-via-delleuropa-su-regole-e-investimenti/>

AI4Business, Boldrini N., *Reti neurali: cosa sono e a cosa servono*, 23 aprile 2022, <https://www.ai4business.it/intelligenza-artificiale/deep-learning/reti-neurali/>



Artificial Intelligence (AI) Ethics: Ethics of AI and Ethical AI, marzo 2020,

<https://www.researchgate.net/publication/340115931>

Attualità parlamento europeo, *Che cos'è l'intelligenza artificiale e come viene usata?*, 3 settembre 2020, aggiornato il 29 marzo 2021,

<https://www.europarl.europa.eu/news/it/headlines/society/20200827STO85804/che-cos-e-l-intelligenza-artificiale-e-come-viene-usata>

BBC, *Artificial intelligence: Google's AlphaGo beats Go master Lee Se-dol*, 26 marzo 2016,

<https://www.bbc.com/news/technology-35785875>

BBC, *DeepMind's AI agent MuZero could turbocharge YouTube*, 23 dicembre 2020,

<https://www.bbc.com/news/technology-55403473>

Benanti P., *“Le AI come uomini: intuitive ma con pregiudizi”*, 2018,

<https://www.paolobenanti.com/post/2018/09/09/ai-pregiudizi>

Cambridge Dictionary, *“Artificial intelligence”*,

<https://dictionary.cambridge.org/dictionary/english-italian/artificial-intelligence>

Chiarelli M., *La sfida della regolazione europea dell'intelligenza artificiale*, 20 dicembre

2019, <https://www.diritto.it/la-sfida-della-regolazione-europea-dellintelligenza-artificiale/>

Choi Q. C., *Protecting Privacy in Surveillance Video While Mining It for Data: A new technique may help defend privacy while permitting useful analysis of surveillance data*, 19

aprile 2022, <https://spectrum.ieee.org/surveillance-privacy#toggle-gdpr>

CNN, Petroff. A., *“Google CEO: AI is 'more profound than electricity or fire'”*, 24 gennaio

2018, <https://money.cnn.com/2018/01/24/technology/sundar-pichai-google-ai-artificial-intelligence/index.html>

Commission of the European Communities, *Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, 15 ottobre 1992, p. 26, <https://aei.pitt.edu/10375/1/10375.pdf>

Commissione europea, *Allegati della proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, 21 aprile 2021, Allegato III, p. 4; [https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0006.02/DOC\\_2&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0006.02/DOC_2&format=PDF)

Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni - Plasmare il futuro digitale dell'Europa*, COM(2020) 67 final, 19 febbraio 2020, <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52020DC0067&from=IT>

Confederazione Svizzera - Dipartimento Federale degli Affari Esteri, *"Intelligenza artificiale e regolamentazione internazionale – Rapporto all'attenzione del Consiglio Federale"*, 13 aprile 2022, <https://www.newsd.admin.ch/newsd/message/attachments/71098.pdf>

Confederazione Svizzera, *Strategia Cina 2021-2024*, 19 marzo 2021, [https://www.eda.admin.ch/dam/eda/it/documents/publications/SchweizerischeAussenpolitik/Strategie\\_China\\_210319\\_IT.pdf](https://www.eda.admin.ch/dam/eda/it/documents/publications/SchweizerischeAussenpolitik/Strategie_China_210319_IT.pdf)

Consiglio d'Europa, *Ad Hoc Committee on Artificial intelligence*, 11 settembre 2019, [https://search.coe.int/cm/Pages/result\\_details.aspx?ObjectId=09000016809737a1](https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016809737a1)

Consiglio europeo, *Riunione speciale del Consiglio europeo (1° e 2 ottobre 2020) – Conclusioni*, 2 ottobre 2020, <https://www.consilium.europa.eu/media/45923/021020-euco-final-conclusions-it.pdf>

Corte europea dei diritti dell'uomo, *Guida all'articolo 8 - Diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza*, aggiornata al 31 agosto 2019, [https://www.echr.coe.int/documents/guide\\_art\\_8\\_ita.pdf](https://www.echr.coe.int/documents/guide_art_8_ita.pdf)

Cullen D., *Why Artificial Intelligence Is Already a Human Rights Issue*, Oxford Human Rights Hub, 31 dicembre 2018, <http://ohrh.law.ox.ac.uk/why-artificial-intelligence-is-already-a-human-rights-issue/>,

European Data Protection Board, *Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR*, 7 luglio 2021, [https://edpb.europa.eu/system/files/2022-02/eppb\\_guidelines\\_202007\\_controllerprocessor\\_final\\_it.pdf](https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_it.pdf)

European Parliamentary Research Service, Scientific Foresight Unit (STOA), PE 641.530, *The impact of the General Data Protection Regulation (GDPR) on Artificial intelligence*, giugno 2020, p. 49, [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS\\_STU\(2020\)641530\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf)

Forbes, Dowson, L. *The law of disruption occupies Wall Street*, ottobre 2011, <https://www.forbes.com/sites/larrydownes/2011/10/16/the-law-of-disruption-occupies-wall-street/?sh=3468b3ef4ebb>

Forbes, Meisner B., *What is the future of artificial intelligence in photo editing?*, 20 gennaio 2020, <https://www.forbes.com/sites/forbesbusinesscouncil/2022/01/20/what-is-the-future-of-artificial-intelligence-in-photo-editing/?sh=238192a7547c>

FRA – European Union Agency for fundamental rights, *Article 8 – Protection of personal data*, <https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data#explanations>

Garante per la protezione dei dati personali, *Autorizzazione generale n. 1/2016: Trattamento dei dati sensibili nei rapporti di lavoro*, 15 dicembre 2016,

<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/5800451>

Garante per la protezione dei dati personali, *Coronavirus: Garante Privacy, no a iniziative "fai da te" nella raccolta dei dati. Soggetti pubblici e privati devono attenersi alle indicazioni del Ministero della salute e delle istituzioni competenti*, Roma, 2 marzo 2020,

<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9282117>

Garante per la protezione dei dati personali, *Documento di indirizzo "Vaccinazione nei luoghi di lavoro: indicazioni generali per il trattamento dei dati personali"*, 13 maggio 2021,

<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9585300>

Garante per la protezione dei dati personali, *Il garante*,

<https://www.garanteprivacy.it/home/autorita>

General Assembly of the United Nations, *Disarmament and International Security (First Committee)*, <http://www.un.org/en/ga/first/>

Goodrich J., IEEE Spectrum, *How IBM's Deep Blue Beat World Champion Chess Player Garry Kasparov The supercomputer could explore up to 200 million possible chess positions per second with its AI program*, 26 gennaio 2021, <https://spectrum.ieee.org/how-ibms-deep-blue-beat-world-champion-chess-player-garry-kasparov>

GPAI, *The Global partnership on Artificial Intelligence*, <https://gpai.ai/about/>

High-Level Expert Group on Artificial Intelligence, *A definition of Artificial Intelligence: main capabilities and scientific disciplines*, Brussels, 18 dicembre 2018,

[https://ec.europa.eu/futurium/en/system/files/ged/ai\\_hleg\\_definition\\_of\\_ai\\_18\\_december\\_1.pdf](https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf)

Hughes A., *ChatGPT: Everything you need to know about OpenAI's GPT-3 tool*, 2 febbraio 2023, <https://www.sciencefocus.com/future-technology/gpt-3/>

IEEE, *Ethically Aligned Design*, 13 dicembre 2016, [https://standards.ieee.org/wp-content/uploads/import/documents/other/ead\\_v1.pdf](https://standards.ieee.org/wp-content/uploads/import/documents/other/ead_v1.pdf)

IEEE, *The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems*, <https://standards.ieee.org/industry-connections/ec/autonomous-systems/>

ITU, *AI for Good Global Summit*, 15 maggio 2018, <https://www.itu.int/en/ITU-T/AI/2018/Pages/default.aspx>

ITU, *Artificial Intelligence*, <https://www.itu.int/en/ITU-T/AI/Pages/default.aspx>

ITU, *Focus Group on Machine Learning for Future Networks including 5G*, <https://www.itu.int/en/ITU-T/focusgroups/ml5g/Pages/default.aspx>

ITU, *Whitepaper for the ITU/WHO Focus Group on Artificial Intelligence for Health*, [https://www.itu.int/en/ITU-T/focusgroups/ai4h/Documents/FG-AI4H\\_Whitepaper.pdf](https://www.itu.int/en/ITU-T/focusgroups/ai4h/Documents/FG-AI4H_Whitepaper.pdf)

Nannini, L., *Possibili Rischi per la Strategia Italiana sull'Intelligenza Artificiale a Confronto con l'EU AI Act*, 29 dicembre 2021, p. 9 [https://www.privacy-network.it/wp-content/uploads/2021/12/Regolamentazioni\\_AI\\_in\\_ITA\\_EU-7.pdf](https://www.privacy-network.it/wp-content/uploads/2021/12/Regolamentazioni_AI_in_ITA_EU-7.pdf)

OECD, *Recommendation of the Council on Artificial Intelligence*, 22 maggio 2019, <https://oecd.ai/en/assets/files/OECD-LEGAL-0449-en.pdf>

Office of Management & Budget, Exec. Office of the President, 17 novembre 2020, “*Guidance for Regulation of Artificial Intelligence Applications*”, <https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf>

OpenAI, *ChatGPT: Optimizing Language Models for Dialogue*, 30 novembre 2022, <https://openai.com/blog/chatgpt/>

Oxford Learner's Dictionaries, "*Artificial intelligence*", <https://www.oxfordlearnersdictionaries.com/definition/english/artificial-intelligence>

Parlamento europeo, *Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale*, 20 ottobre 2020, [https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276\\_IT.html](https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_IT.html)

Partnership on AI, <https://partnershiponai.org/partners/>

Privacy.it, *Gli USA pressano la UE: no a normazione rigida su intelligenza artificiale*, 8 gennaio 2020, <https://www.privacy.it/2020/01/08/usa-normazione-intelligenza-artificiale/>

Rappresentanza Permanente d'Italia ONU – Ginevra, *La Convenzione su certe armi convenzionali e Protocolli annessi*, <https://italiarappginevra.esteri.it/rappginevra/it/il-disarmo/trattati-e-convenzioni/armi-conv-effetti-indiscriminati.html>

Rappresentanza Permanente d'Italia ONU – Ginevra, *La Prima Commissione dell'Assemblea Generale dell'ONU*, <https://italiarappginevra.esteri.it/rappginevra/it/il-disarmo/la-prima-commissione-dell-assemblea/>

Science, Hutson M., *How Researchers Are Teaching AI to Learn Like a Child*, Science, 24 maggio 2018, <https://www.sciencemag.org/news/2018/05/how-researchers-are-teaching-ai-learn-child>

Strickland E., *The turbulent past and future of artificial intelligence*, 30 settembre 2021, <https://spectrum.ieee.org/history-of-ai>

TechTarget, Labbe M., Wigmore I., “*narrow AI (weak AI)*”, agg. giugno 2021, <https://www.techtarget.com/searchenterpriseai/definition/narrow-AI-weak-AI#:~:text=Narrow%20AI%2C%20also%20known%20as,intelligence%20for%20a%20dedicated%20purpose>

The Artificial Intelligence Act, <https://artificialintelligenceact.eu/>

United Nations Interregional Crime and Justice Research Institute, *Centre on Artificial Intelligence and Robotics*, [http://www.unicri.it/topics/ai\\_robotics/centre](http://www.unicri.it/topics/ai_robotics/centre)

United Nations Sustainable Development Blog, *The Future of Everything – Sustainable Development in the Age of Rapid Technological Change*, 9 ottobre 2017, <https://www.un.org/sustainabledevelopment/blog/2017/10/looking-to-future-un-to-consider-how-artificial-intelligence-could-help-achieve-economic-growth-and-reduce-inequalities/>

WP29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, 3 ottobre 2017, aggiornato il 6 febbraio 2018, p. 10, [http://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=612053](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053)

WP29, *Opinion 03/2013 on purpose limitation*, 2 aprile 2013, p. 35, [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf)

WP29, *Opinion 05/2014 on Anonymisation Techniques*, 10 aprile 2014, p. 20, [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf)

WP29, *Opinion 1/2010 on the concepts of "controller" and "processor"*, 16 febbraio 2010, [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf)

WP29, *Opinion 4/2007 on the concept of personal data*, 20 giugno 2007, p. 18,

[https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf)



## **Riferimenti normativi e giurisprudenza**

CEPEJ, *Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi*, Introduzione, p. 5

Consiglio d'Europa, *Convenzione Europea dei diritti dell'uomo*, 1950, art. 8

*Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*, Strasburgo, Traduzione ufficiale della Cancelleria federale della Svizzera, 28 gennaio 1981

L. 300/1970 (Statuto dei Lavoratori), Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento, art. 4

**Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati**

Direttiva 95/46/CE, art. 2, par. 1, lett. h)

Direttiva 95/46/CE, art. 3

Direttiva 95/46/CE, art. 5

Direttiva 95/46/CE, art. 29

Direttiva 95/46/CE, art. 30

Direttiva 1997/66/CE del Parlamento europeo e del Consiglio del 15 dicembre 1997 sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni

Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)

L. n. 675 del 31 dicembre 1996 - *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*

Trattato che istituisce la Comunità europea (versione consolidata Maastricht), Parte sesta: Disposizioni generali e finali, gazzetta ufficiale n. C 340 del 10/11/1997 pag. 0294 - versione consolidata, art. 286

Decreto legislativo 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali*

Carta dei diritti fondamentali dell'Unione europea, 2000/C 364/01, art. 52, par. 1

Trattato sul funzionamento dell'Unione europea (versione consolidata), art. 16, commi I e II

Trattato sull'Unione europea (versione consolidata), art. 39

Trattato sul funzionamento dell'Unione europea (versione consolidata), art. 114.1

**Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016  
relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati  
personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE  
(regolamento generale sulla protezione dei dati)**

Regolamento 2016/679, Considerando 2

Regolamento 2016/679, Considerando 4

Regolamento 2016/679, Considerando 15

Regolamento 2016/679, Considerando 39

Regolamento 2016/679, Considerando 40

Regolamento 2016/679, Considerando 60

Regolamento 2016/679, Considerando 71

Regolamento 2016/679, Considerando 74

Regolamento 2016/679, art. 4, comma I, nn. 2, 3, 13, 11, 14, 15

Regolamento 2016/679, art. 6, comma III.

Regolamento 2016/679, art. 7

Regolamento 2016/679, art. 9, comma I, lett. b) e d)

Regolamento 2016/679, art. 9, comma II, lett. i) e j)

Regolamento 2016/679, art. 22, commi I, II e IV.

Regolamento 2016/679, art. 23

Regolamento 2016/679, art. 28

Regolamento 2016/679, art. 35

Regolamento 2016/679, art. 38

Regolamento 2016/679, art. 89, comma I

**Commissione europea, Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, 2021/0106 (COD), Bruxelles, 21 aprile 2021**

AI Act, Considerando 1

AI Act, Considerando 3

AI Act, Considerando 7

AI Act, Considerando 8

AI Act, Considerando 11

AI Act, Considerando 16

AI Act, Considerando 17

AI Act, Considerando 23

AI Act, Considerando 32

AI Act, comb. disp. dei consideranda 53, 58, 64

AI Act, Considerando 84

AI Act, art. 2, comma I

AI Act, art. 3, comma I

AI Act, art. 5

AI Act, art. 6

AI Act, art. 10, commi I e V

AI Act, art. 14

AI Act, art. 17

AI Act, art. 33, commi III, VIII e IX

AI Act, art. 34, commi I e II

AI Act, art. 43

AI Act, art. 48, comma IV

AI Act, art 71

AI Act, art. 72

Corte europea dei diritti dell'uomo, *Denisov c. Ucraina*, para. 111-112, 25 settembre 2018.

C-311/18, *Data Protection Commissioner c. Facebook Ireland Ltd., Maximilian Schrems*, 16 luglio 2020.

C-131/12, *Google Spain*, para. 34.

C-210/16, *Wirtschaftsakademie*, para. 28.

C-40/17, *Fashion ID*, para. 65–66.