Università degli studi di Padova

Dipartimento di Diritto Privato e Critica del Diritto

Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea Magistrale in

Giurisprudenza

a.a. 2022/2023

INTELLIGENZA ARTIFICIALE E DIRITTO: L'APPROCCIO DELL'UNIONE EUROPEA

Relatore: Chiar.mo Professore Sarra Claudio

Laureando: Mihai Jignea

Matricola: 1147812

INDICE:

INTRODUZIONE - La nascita dell'IA e l'approccio dell'Unione Europea…….7

CAPITOLO I – IA E DIRITTO……...13

1. LA REGOLAMENTAZIONE DELL'IA A LIVELLO INTERNAZIONALE…..13

A. Cina e IA……..13

B. Usa e IA……...14

C. UE e IA ……...14

2. LA DEFINIZIONE DI INTELLIGENZA ARTIFICIALE……..22

3. CONCETTI FONDAMENTALI NELL'IA: DEFINIZIONI CHIAVE……..26

A. Machine Learning……....26

B. Big Data……...29

C. IA forte e IA debole…….31

CAPITOLO II - IL GDPR:……..33

1. IL DIRITTO ALLA PRIVACY……...33

A. La nascita del diritto alla privacy……33

B. Il diritto alla privacy nella Dichiarazione Universale dei Diritti Umani…….34

C. Il diritto alla privacy nella Convenzione Europea dei Diritti dell'Uomo……35

2. LA LEGISLAZIONE COMUNITARIA IN RELAZIONE ALLA PROTEZIONE DEI DATI PERSONALI: Verso il GDPR……..37

A. La Direttiva 95/46/CE…….37

B. Il regolamento CE 45/2001 sulla protezione dei dati……..38

3. IL GDPR……...40

A. Oggetto e finalità…….41

B. L'ambito di applicazione materiale…….44

C. L'ambito di applicazione territoriale……...46

4. I PRINCIPI DEL GDPR APPLICABILI AL TRATTAMENTO DEI DATI…...52

A. I principi di liceità, correttezza e trasparenza…….....52

B. Il principio della finalità nel trattamento dei dati……...55

C. Ulteriori principi: minimizzazione dei dati, conservazione e accuratezza…….57

4.1. I diritti dell'interessato…….....58

A. Il diritto all'informazione……....59

B. Il diritto d'accesso……...60

C. Il diritto all'oblio…….....60

D. Il diritto di opposizione……..64

E. Il diritto alla portabilità dei dati……..65

4.2 Gli obblighi e le responsabilità del titolare e del responsabile del Trattamento…….68

A. Il titolare e il responsabile del trattamento: le definizioni del GDPR……...68

B. Gli obblighi principali……...71

C. La valutazione d'impatto……..72

D. Privacy by design e privacy by default……....73

E. Il DPO (Data Protection Officer)…….75

CAPITOLO III - L'AI ACT:……...79

1. LE FONTI DELL'AI ACT……..80

2. LA SUA STRUTTURA…….....82

3. LA DEFINIZIONE DI IA SECONDO L'AI ACT……87

4. LE PRATICHE DI INTELLIGENZA ARTIFICIALE VIETATE……89

A. Manipolazione……89

B. Sfruttamento di gruppi vulnerabili……..91

C. Social scoring pubblico……...93

D. Identificazione biometrica remota e in tempo reale……...94

5. SISTEMI IA AD ALTO RISCHIO…….....96

A. Dati e governance dei dati……..97

B. Trasparenza e fornitura di informazioni agli utenti…….....98

C. Supervisione umana……..100

6. SISTEMI IA A BASSO RISCHIO……...101

7. VALUTAZIONE DI CONFORMITÀ, MONITORAGGIO E IL RUOLO DELLE AUTORITÀ PUBBLICHE……...102

8. INTELLIGENZA ARTIFICIALE E RESPONSABILITÀ CIVILE……...105

CONCLUSIONI…….111

BIBLIOGRAFIA……....115

INTRODUZIONE - La nascita dell'IA e l'approccio dell'Unione Europea

L'intelligenza artificiale (indicata anche con la sigla “IA”, o in inglese “AI”) è certamente una delle più importanti innovazioni tecnologiche del nostro tempo, in grado di influenzare e di farsi influenzare da numerose discipline, fra le quali la filosofia, la matematica, l'economia, il diritto, le neuroscienze, la psicologia, la cibernetica, le scienze cognitive e la linguistica.[1] Volendo individuare il momento della nascita dell'IA, questo viene fatto coincidere con il 1956 anno del famoso seminario estivo tenutosi presso il Dartmouth College di Hanover nel New Hampshire durante il quale la nuova disciplina viene fondata programmaticamente a partire dalla raccolta dei contributi sviluppati negli anni precedenti e in direzione delle potenzialità future. Questa data di nascita individuata convenzionalmente dalla comunità scientifica come punto di origine dell'IA, tuttavia, non può non essere collegata anche agli sviluppi tecnologici pregressi che hanno tracciato la strada da seguire da un punto di vista tecnologico. A sostegno di ciò è bene ricordare il saggio del 1937 intitolato "*On Computable Numbers, with an Application to the Entscheidugsproblem*" ad opera di Alan Mathison Turing[2] (1912 - 1954), all'epoca un giovane matematico dell'Università di Cambridge ed oggi considerato l'inventore del computer. Questo saggio oltre che avere un'incidenza pratica dal punto di vista dello sviluppo tecnologico ha avuto anche un'importanza notevole nello studio teorico dell'IA

[1] Somalvico M.; 1987 *“L’Intelligenza artificiale”,* Rusconi, Milano

[2] Cfr. Wikipedia Alan Turing - Wikipedia ; Alan Turing, figura di spicco nel panorama storico e scientifico del XX secolo, ha lasciato un segno indelebile nella storia dell'informatica e dell'intelligenza artificiale. Il suo contributo più noto è stato il ruolo cruciale che ha svolto nella decodifica del codice Enigma durante la Seconda Guerra Mondiale, un'impresa che ha contribuito in modo significativo alla vittoria degli Alleati. Tuttavia, il suo genio e la sua influenza vanno ben oltre questo tragico conflitto. Turing è riconosciuto come il padre della scienza informatica grazie alla sua creazione della 'macchina di Turing', un concetto teorico che ha posto le basi per la moderna elaborazione automatizzata delle informazioni e per lo sviluppo dei primi computer.
L'importanza di Turing nel mondo dell'informatica si estende anche all'intelligenza artificiale. Il suo celebre saggio del 1950, 'Computing Machinery and Intelligence', ha proposto il famoso 'test di Turing' come misura di intelligenza in una macchina. Questo concetto ha suscitato dibattiti e riflessioni su ciò che significa essere intelligenti e su come le macchine possano simulare questa intelligenza. Il suo lavoro ha gettato le basi per l’era digitale e l’intelligenza artificiale.

introducendo da un lato il moderno paradigma per il quale la conoscenza è un processo che si sviluppa attraverso ipotesi sempre provvisorie e incomplete e, dall'altro lato, il definitivo abbandono dell'impostazione di Gottfried Leibniz (1646-1716) che nel Seicento aveva sostenuto che una macchina universale avrebbe potuto dare all'uomo conclusive verità e certezze, trasformando il ragionamento in calcolo[3]. Turing più che voler costruire uno strumento che permetta all'uomo di perseguire il vero, puntava alla creazione di una macchina che mediante la logica matematica fosse in grado di organizzare razionalmente le informazioni e di elaborarle in modo logico, sequenziale, computazionale. Il contenuto di questo saggio, al quale solo nei decenni successivi rispetto alla sua pubblicazione venne riconosciuta l'importanza che merita venendogli attribuita la definizione di "*Manifesto dell'intelligenza artificiale*", trova assoluto riscontro pratico nelle opere ingegneristiche poste in essere tra il 1939 e il 1945 da Alan Turing e i suoi collaboratori per il GCCS (*Government Code and Cypher School*) il Centro dei servizi segreti inglesi di decodifica delle comunicazioni criptate dell'esercito tedesco, che aveva sede a Bletcheley Park a nord di Londra. Proprio il contesto bellico e dunque la necessità di difendersi delle forze alleate dalle truppe naziste, permise di confluire risorse materiali e umane nello sviluppo di nuove tecnologie che portarono (sotto la direzione di Alan Turing) dapprima alla costruzione del *Colussus*[4] (1943) e poi del *Mark 1*[5]

[3] Viterbo A.; Dir. informatica, fasc.4-5, 2007, pag. 725

[4] Cfr. Wikipedia Colossus - Wikipedia; Il Colossus è un'icona dell'innovazione tecnologica e della dedizione intellettuale, rappresenta un contributo epocale di Alan Turing al panorama della crittografia e dell'informatica. Ideato durante la Seconda Guerra Mondiale come risposta alla crescente sfida posta dal sistema di cifratura tedesco Lorenz, il Colossus è stata la prima macchina programmabile elettronica a essere costruita.
L'ingegnosità di Turing ha plasmato il Colossus, grazie al quale è stato possibile decifrare messaggi cifrati in modo più rapido ed efficace rispetto ai metodi tradizionali. Questa macchina ha avuto un impatto cruciale sullo svolgimento del conflitto, contribuendo alla vittoria degli Alleati attraverso la rivelazione di comunicazioni nemiche precedentemente inaccessibili.
Il successo del Colossus ha gettato le basi per il futuro sviluppo delle moderne tecnologie informatiche, influenzando direttamente l'evoluzione dei computer elettronici. La sua architettura innovativa e la visione di Turing sulla potenza dell'elaborazione automatizzata dei dati hanno tracciato una strada per le generazioni future di calcolatori elettronici e hanno plasmato il mondo digitale in cui viviamo oggi.

[5] Cfr. Wikipedia Harvard Mark I - Wikipedia; Il Mark I, frutto della visione ingegnosa di Alan Turing, costituisce un pilastro fondamentale nella storia dell'informatica e nella rivoluzione tecnologica. Progettato e sviluppato durante gli anni della Seconda Guerra Mondiale, il Mark I rappresenta uno dei primi computer elettronici di grande scala. IL Mark I sfruttava il concetto di una macchina universale di elaborazione. Questo

(1948) considerato il primo computer universale della storia. Al termine poi della Seconda guerra mondiale questo sviluppo tecnologico si sposterà del campo militare a quello civile.

L'individuazione del 1956 come anno di nascita dell'IA, nonostante appunto le importanti innovazioni avvenute anche precedentemente a tale data, è dovuta anche al fatto che in tale anno, proprio in occasione del sopra citato seminario presso il Dartmouth College di Hanover nel New Hampshire, avvenne la coniazione del termine "*Intelligenza Artificiale*" ad opera dello scienziato John McCarthy. Secondo lo studioso, "T*he Artificial Intelligence It is the science and engineering of making intelligent machines, especially intelligent computer programs*"[6] («*L'Intelligenza Artificiale è la scienza e l'ingegneria della creazione di macchine intelligenti, in particolare di programmi informatici intelligenti*.»). Ecco dunque che pur essendo questa una definizione non ancora esaustiva per definire un'IA, essa rappresenta comunque un punto di svolta decisivo nello sviluppo di questa tecnologia permettendo così di individuare il 1956 come anno di nascita dell'Intelligenza Artificiale. A partire poi da questa data il percorso di crescita delle tecnologie di IA è stato segnato da alcune emblematiche conquiste, le quali vengono ricordate in particolare per l'incisivo impatto mediatico che le ha contraddistinte. Nella ricostruzione dell'evoluzione dell'IA si ricordano i successi del programma Deep Blue, che nel 1997 fu in grado di sconfiggere il campione mondiale di scacchi Garry Kasparov; dell'auto Stanley, prima auto a guida autonoma, che nel 2005 riuscì a vincere una gara di guida autonoma nel deserto americano; del programma Watson, che nel 2011 riuscì a sconfiggere il campione del programma televisivo americano Jeopardy!; fino ad arrivare alle odierne

innovativo calcolatore ha dimostrato la sua versatilità attraverso l'elaborazione di calcoli complessi, sostenendo la decrittazione di codici crittografici e contribuendo al progresso delle attività di intelligence durante il conflitto.
Oltre al suo impatto durante la guerra, il Mark I ha aperto la strada all'era dei computer elettronici, gettando le basi per le future innovazioni nell'informatica e nella tecnologia. La sua architettura pionieristica e il contributo di Turing hanno contribuito alla nascita di un nuovo mondo di calcolo automatico e rappresentano una tappa cruciale nel percorso evolutivo dei computer moderni.

[6] McCathy J.; "*What is Artificial Intelligence"*, 2007, reperibile in: http://www-formal.stanford.edu/jmc/whatisai.pdf

applicazioni nell'ambito della robotica (industriale, sanitaria, automobilistica) e dei servizi digitali (servizi di GPS, assistenti vocali, riconoscimento immagini, servizi di profilazione). Il passaggio che ha segnato il successo dell'IA coincide con lo sviluppo del ML (Machine Learning)[7] e la nascita dei Big Data[8], la cui combinazione ha reso non più necessario che fosse l'operatore a fornire tutta la conoscenza preliminare al sistema artificiale perché questi elaborasse l'output desiderato, ma i sistemi di ML sono impostati assegnando loro un determinato compito e ricevendo una grande quantità di dati da utilizzare come esempi di come questo compito può essere realizzato o da cui ricavare modelli.[9]

Questo rapido e incessante sviluppo ha portato l'IA a penetrare sempre di più nella vita quotidiana delle persone e in numerosi settori d'attività suscitando però d'altro canto anche un ampio dibattito in relazione alle implicazioni giuridiche legate al funzionamento e all'utilizzo dell'intelligenza artificiale. Ecco che dunque questo elaborato cercherà in particolare di analizzare le modalità e gli strumenti adottati dall'Unione Europea in relazione alle sfide che l'IA propone; verranno così prese in considerazione le varie tappe legislative seguite dall'UE in relazione all'intelligenza artificiale sino a giungere alla recente pubblicazione di una proposta di Regolamento dell'Unione Europea che si prefigge di stabilire regole armonizzate, il c.d. *Artificial Intelligence Act* (AI Act). Si tratta di una proposta di notevole impatto destinata ad

[7] Cfr. Panattoni B.; Diritto dell'Informazione e dell'Informatica (Il), fasc.2, 1 aprile2021, p. 317; L'idea fondamentale dietro il machine learning è l'elaborazione automatizzata dei dati per identificare correlazioni e tendenze. Utilizzando algoritmi appositi, i computer analizzano i dati di addestramento e ne estraggono modelli di comportamento. Questi modelli vengono quindi applicati a nuovi dati per fare previsioni o prendere decisioni. Attraverso l'iterativo processo di apprendimento, il machine learning consente alle macchine di migliorare costantemente le loro prestazioni e adattarsi a situazioni mutevoli, rendendolo uno strumento fondamentale nella risoluzione di problemi complessi e nello sviluppo di soluzioni intelligenti.

[8] Cfr, Agata C.; "*Intelligenza artificiale, big data e nuovi diritti*", fascicolo 1-2022 Rivista Italiana di informatica e diritto, p. 94-97 ; Si tratta di insiemi di dati di dimensioni enormi e complessi, che richiedono strumenti avanzati per essere gestiti, analizzati e compresi.
La caratteristica principale dei big data è la loro vastità. Questi dati provengono da diverse fonti, tra cui social media, sensori, transazioni finanziarie e dispositivi connessi, generando un flusso costante di informazioni. La varietà dei dati è altrettanto rilevante: testo, immagini, audio, video e dati strutturati si combinano per offrire un panorama completo delle attività umane e dei processi. big data hanno rivoluzionato numerosi settori, dalla scienza e l'industria all'assistenza sanitaria e al marketing. Tuttavia, la gestione etica e la protezione della privacy sono questioni cruciali legate ai big data, poiché l'ampio accesso a queste informazioni solleva interrogativi sull'uso responsabile e la tutela dei diritti individuali.

[9] Panattoni B.; Diritto dell'Informazione e dell'Informatica (Il), fasc. 2, 1 aprile 2021, p. 317

erigersi a punto di riferimento per la successiva regolamentazione normativa in relazione all'IA, cercando di garantire un sistema di tutele che sia certo, uniforme e proporzionato. Inoltre, se da un lato l'attenzione per la tutela dei soggetti che si relazionano con l'IA è sicuramente uno degli obbiettivi principali dell'AI Act, dall'altro lato il Regolamento è attento anche a non impedire lo sviluppo stesso della tecnologia adottando dunque un approccio che garantisca che essa possa continuare a crescere nel rispetto però di diritti fondamentali precedentemente individuati. A sostegno di questo sguardo rivolto al futuro che permetta lo sviluppo dell'IA nonostante le garanzie adottate per i singoli individui è la definizione stessa di Intelligenza Artificiale che il Regolamento adotta: "*software sviluppato con una o più delle tecniche che si trovano elencate nel primo allegato del Regolamento e che può, per un dato insieme di obiettivi definiti dall'uomo, generare output come contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono*."[10] Questa formulazione intende conciliare due diversi obiettivi perseguiti dal Regolamento europeo: da una parte, fornire e garantire un sufficiente grado di certezza giuridica, dall'altra, caratterizzarsi per una certa flessibilità e capacità di adeguamento per rimanere al passo con la rapida evoluzione che segna lo sviluppo delle tecnologie di IA: in altre parole, essere "*future-proof*".[11]

Indispensabile poi per meglio comprendere la disciplina giuridica adottata dall'UE in tema di IA è l'analisi che di seguito verrà fatta in merito al GDPR, analizzando come i principi predisposti in materia di trattamento dei dati da quest'ultimo si intreccino con la realtà e le regole dell'Intelligenza Artificiale predisposti dall'AI Act.

L'elaborato porterà anche ad analizzare il tema della responsabilità in tema d'Intelligenza Artificiale, affrontato non tanto dall'IA Act quanto dalle discipline precedenti alla sua

[10] Art. 3 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
[11] Panattoni B.; Diritto dell'Informazione e dell'Informatica (Il), fasc.2, 1 aprile 2021, p. 317

introduzione, come ad esempio la disciplina della Responsabilità per danno da prodotto difettoso o la Risoluzione del Parlamento europeo concernente la responsabilità civile dell'IA del 2020 che contiene una proposta di regolamento sulla materia volta a regolamentare la responsabilità civile. Tutto questo ovviamente solleva ulteriori numerosi dibattiti sociali e giuridici sull'utilizzo attuale e futuro dell'IA che verranno affrontati nel corso di questa dissertazione.

CAPITOLO I – IA E DIRITTO

1. LA REGOLAMENTAZIONE DELL'IA A LIVELLO INTERNAZIONALE

In un'era sempre più digitale come la nostra, dove su base quotidiana veniamo in contatto con sistemi intelligenti, la creazione di un framework normativo in grado da un lato di tutelare i soggetti che entrano in contatto con tali tecnologie e dall'altro di favorire comunque lo sviluppo di queste ultime, è certamente uno degli obbiettivi primari da perseguire. Se da un punto di vista prettamente tecnologico l'IA non ha barriere o confini geografici e politici e la si può dunque considerare come un mercato globale, da un punto di vista normativo invece tale mercato appare sostanzialmente diviso in tre aree di influenza: quella europea, quella statunitense e quella cinese.

A) Cina e IA

Per quanto riguarda il modello adottato in Cina esso appare come un modello dirigistico basato sul capitalismo di Stato. Certamente la Cina si caratterizza per essere sempre più attiva anche nella produzione di norme: nell'ambito della protezione dei dati personali, basti ricordare la *Personal Information Protection Law* (PIPL) in vigore dal 1° novembre 2021,[12] la *Data Security Law* (DSL) in vigore dal 1° settembre 2021[13] e la *Cybersecurity Law* (CSL) in vigore dal 1° giugno 2021.[14] Sotto il profilo strategico, la recente creazione della *Shanghai Data Exchange* (SDE), la borsa di Shanghai per lo scambio dei dati, persegue anche l'obiettivo di creare lo "*Shanghai Model*" per la compravendita di dati. Il "modello Shanghai" ha l'ambizione

[12] Personal Information Protection Law of the People's Republic of China, 20 agosto 2021
[13] Data Security Law of the People's Republic of China, 10 giugno 2021
[14] Cybersecurity Law of the People's Republic of China, 6 novembre 2016

di risolvere i problemi che oggi rendono difficile la circolazione dei dati e di proporsi come modello globale di riferimento per eliminare i rischi dell'incertezza giuridica.[15]

B) USA e IA

Negli USA invece abbiamo disposizioni legislative sia a livello statale che a livello federale. Da quest'ultimo punto di vista uno dei primi documenti in materia è il *Future of Artificial Intelligence Act of 2017*[16] il cui intento è quello di analizzare i rischi e benefici che possono portare lo sviluppo dell'IA per la società e per l'economia statunitense. Da un punto di vista dei singoli Stati l'attenzione legislativa si è rivolta in particolare ai veicoli a guida autonoma con lo Stato del Nevada che, nel 2011, è stato il pioniere in questo ambito ammettendo la possibilità che in presenza di determinate condizioni questi i veicoli possano essere testati per circolare sulle strade dello Stato.[17] Successivamente anche ulteriori Stati come Arizona, Illinois, Minnesota sono intervenuti in materia indirizzandosi sulla stessa rotta indicata dallo Stato del Nevada.

C) Unione Europea e IA

L'Unione Europea ha adottato un modello cosiddetto regolatorio, intendendosi per questo non soltanto normare e disciplinare i nuovi fenomeni, le nuove tecnologie e i nuovi beni, ma anche fare sì che il modello europeo divenga un riferimento globale e possa essere adottato nelle altre regioni geopolitiche.[18] L'UE fin da quando ha compreso l'importanza e l'impatto che queste nuove tecnologie hanno nei confronti dell'essere umano e della sua vita, ha sempre cercato di creare un apparato normativo che tenga conto soprattutto delle implicazioni umane ed etiche

[15] Finocchiaro G.; Diritto dell'Informazione e dell'Informatica (Il), fasc.2, 1 aprile 2022, p. 303
[16] U.S. Congress, Senate, "*Future of Artificial Intelligence Act of 2017*", S 2217, 115th Cong., 63 1st sess., introduced in Senate December 12, 2017, disponibile presso https://www.congress.gov/bill/115th-congress/senate-bill/2217/text
[17] Jann Stinnesbeck, Research Division Legislative Counsel Bureau, "*Research Brief On 65Autonomous Vehicles*" (Novembre 2017), disponibile online presso https://www.leg.state.nv.us/Division/Research/Publications/ResearchBriefs/AutonomousVehicles.pdf
[18] Finocchiaro G.; Diritto dell'Informazione e dell'Informatica (Il), fasc.2, 1 aprile 2022, p. 303

emergenti nell'era digitale.[19] In ragione di ciò sono state intraprese varie azioni volte a creare un regolamento più chiaro e completo possibile per affrontare le problematiche sociali e giuridiche emerse in tale ambito. Ecco che dunque con la **Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica**, rubricata come *Norme di diritto civile sulla robotica*, si è posta l'attenzione su tematiche che, partendo dalla letteratura e dalla fantascienza, sono approdati all'interno di riflessioni che la società contemporanea comincia ad avvertire come ormai incombenti.[20] Questa Risoluzione nella parte introduttiva, partendo da riflessioni generali sulla robotica e sulle nuove tecnologie in generale, introduce alcune considerazioni avanzate dal Parlamento Europeo su tematiche che riguardano diversi ambiti come quello etico, giuridico, economico, della sicurezza, del lavoro e dell'ambiente. Ecco, dunque, che il Parlamento sottolinea:

- Che l'umanità si trova ora sulla soglia di un'era nella quale robot, bot, androidi e altre manifestazioni dell'intelligenza artificiale sembrano sul punto di avviare una nuova rivoluzione industriale, suscettibile di toccare tutti gli strati sociali, rendendo imprescindibile che la legislazione ne consideri le implicazioni e le conseguenze legali ed etiche, senza ostacolare l'innovazione;
- La necessità di creare una definizione di robot e di IA che sia flessibile e non ostacoli l'innovazione;
- L'impatto positivo che gli sviluppi tecnologici hanno avuto sul tasso di occupazione negli ultimi duecento anni ponendo l'attenzione sul fatto che lo sviluppo dell'IA è in

[19] Cfr. Moro P., "*Intelligenza artificiale e tecnodiritto. Fondamenti etici ed innovazione legislativa"*, in Moro P. (a cura di), "*Etica, Diritto e Tecnologia. Percorsi dell'informatica giuridica contemporanea*", Franco angeli, Milano 2021, pp. 7-24 (p.17)
[20] Di Viggiano P.; "*Etica, Robotica e Lavoro: Profili D'Informatica Giuridica*" vol. 16, no. 22, 2018, p. 247-266

grado di trasformare le abitudini lavorative innalzando i livelli di efficienza, di risparmio, di sicurezza e migliorare il livello dei servizi;

- La necessità di analizzare non solo i vantaggi portati dalle nuove tecnologie ma anche gli svantaggi diretti ed indiretti sulla società nel suo complesso;
- Che i cambiamenti economici derivanti dalle nuove tecnologie devono essere accompagnati da attente riflessioni sul mercato del lavoro, l'istruzione e delle politiche sociali;
- Come lo sviluppo nel campo della robotica e dell'IA debba essere pensato in modo tale da preservare la dignità, l'autonomia e l'autodeterminazione degli individui.

È interessante notare come la Risoluzione nel suo prosieguo affidi all'Unione un ruolo primario a livello globale nella definizione di principi etici fondamentali da rispettare per lo sviluppo, la programmazione e l'utilizzo di robot e dell'intelligenza artificiale, andando così a fare della legislazione dell'Unione una sorta di punto di riferimento al quale gli altri Paesi possano rifarsi.

Altre considerazioni di fondamentale importanza compiute dal Parlamento Europeo in questa Risoluzione riguardano il tema della responsabilità; in tale ambito il Parlamento sottolinea come il fatto che essendo i robot sempre di più dotati di caratteristiche autonome e cognitive che permettono loro di interagire con l'ambiente circostante e modificarlo, porta ad una necessaria rivisitazione della disciplina vigente, perché se è vero che in base all'attuale quadro giuridico, la responsabilità da prodotto (secondo la quale il produttore di un prodotto è responsabile dei malfunzionamenti) e le norme che disciplinano la responsabilità per azioni dannose (in virtù delle quali l'utente di un prodotto è responsabile di un comportamento che conduce al danno) sono applicabili ai danni causati dai robot e dall'intelligenza artificiale, nel momento in cui un'IA prende decisioni autonome le norme tradizionali non sono sufficienti per attivare la responsabilità per i danni causati da un robot, in quanto non consentirebbero di

determinare qual è il soggetto cui incombe la responsabilità del risarcimento né di esigere da tale soggetto la riparazione dei danni causati.

La Risoluzione successivamente individua anche alcuni principi generali riguardanti lo sviluppo della robotica e dell'intelligenza artificiale, invitando anzitutto la Commissione a proporre definizioni europee comuni di sistemi ciberfisici, di sistemi autonomi, di robot autonomi intelligenti e delle loro sottocategorie, prendendo in considerazione le seguenti caratteristiche di un robot intelligente:

- la capacità di acquisire autonomia grazie a sensori e/o mediante lo scambio di dati con il proprio ambiente (interconnettività) e l'analisi di tali dati;
- la capacità di apprendimento attraverso l'esperienza e l'interazione;
- la forma del supporto fisico del robot;
- la capacità di adeguare il suo comportamento e le sue azioni all'ambiente.

Il Parlamento Europeo ritiene poi necessario che venga introdotto un sistema di registrazione dei robot presenti sul mercato dell'UE affidando se necessario tale incarico ad un'agenzia designata dall'UE al fine di monitorare al meglio la presenza dell'IA sul territorio dell'Unione. Si sottolinea successivamente come solo un impianto giuridico proveniente dall'UE possa evitare una frammentazione in materia di IA che risulti dannosa per tutti gli agenti del mercato e per la ricerca e lo sviluppo in campo tecnologico.

Nella parte finale della Risoluzione il Parlamento poi predispone un Codice deontologico per alcuni dei soggetti che operano sul mercato, come ad esempio;

1) **Ricercatori** e i **progettisti**; essi devono agire in modo responsabile, tenendo pienamente conto della necessità di rispettare la dignità, la privacy e la sicurezza delle persone; garantire che la ricerca sulla robotica sia condotta nell'Unione europea in modo

sicuro, etico ed efficace. Essi poi dovrebbero impegnarsi a tenere un comportamento etico e deontologico quanto più rigoroso possibile e a rispettare i seguenti principi:

a) *beneficenza*: i robot devono agire nell'interesse degli esseri umani;
b) *non-malvagità*: la dottrina del *"primum, non nocere*", in virtù della quale i robot non devono fare del male a un essere umano;
c) *autonomia*: la capacità di adottare una decisione informata e non imposta sulle condizioni di interazione con i robot;
d) *giustizia*: un'equa ripartizione dei benefici associati alla robotica e l'accessibilità economica dei robot addetti all'assistenza a domicilio e, in particolare, a quelli addetti alle cure sanitarie.

2) **Comitati Etici di Ricerca (CER)**; Un CER è di norma incaricato di esaminare tutte le attività di ricerca che coinvolgano soggetti (umani) condotte dal personale impiegato all'interno dell'organismo interessato o da quest'ultimo; di assicurare l'indipendenza, la professionalità e la tempestività dell'esame etico; di tutelare la dignità, i diritti e il benessere dei soggetti che partecipano alla ricerca; di tenere in considerazione la sicurezza del ricercatore o dei ricercatori; Tutti gli organismi di ricerca dovrebbero definire opportune procedure per monitorare le attività di ricerca che hanno ottenuto l'approvazione etica fino alla loro conclusione e per garantire una costante verifica se il progetto di ricerca prevede eventuali variazioni nel tempo che potrebbero dover essere trattate. Il monitoraggio dovrebbe essere proporzionato alla natura e al grado di rischio associato alla ricerca. Se un CER ritiene che una relazione di monitoraggio sollevi sostanziali timori circa la conduzione etica dello studio, dovrebbe chiedere un resoconto completo e dettagliato delle ricerche ai fini di una valutazione etica esaustiva. Ove si ritenga che uno determinato studio sia svolto in maniera non etica, è opportuno prendere

in considerazione la possibilità di revocarne l'approvazione ed esigere la sospensione o l'interruzione delle attività di ricerca.

3) Gli **Utenti**;
    a) essi sono autorizzati ad avvalersi di un robot senza rischi né il timore di un danno fisico o psicologico;
    b) hanno il diritto di attendersi che un robot svolga qualsiasi compito per cui è stato espressamente concepito;
    c) non sono autorizzati a utilizzare un robot in alcun modo che sia contrario ai principi e alle norme etiche o giuridiche;
    d) non sono autorizzati a utilizzare un robot in alcun modo che sia contrario ai principi e alle norme etiche o giuridiche.[21]

In seguito a tale Risoluzione si sono susseguiti ulteriori interventi in ambito di IA a livello europeo che hanno cercato sempre di più di stabilire regole e principi di riferimento per le nuove tecnologie. In tal senso possiamo ricordare che con Comunicazione 25 aprile 2018 (*L'intelligenza artificiale per l'Europa*) la Commissione Europea ha esplicitamente favorito e incentivato qualsiasi proposta di regolamentazione necessaria per affrontare le questioni emergenti legati all'IA; nel giugno del 2018 poi venne istituita l'*Alleanza europea per l'intelligenza artificiale*, costituita da una piattaforma destinata a consentire a migliaia di portatori di interessi di discutere in un forum telematico le implicazioni tecnologiche e sociali dell'intelligenza artificiale. Sempre la Commissione Europea ad aprile del 2019 ha approvato i requisiti fondamentali stabiliti negli orientamenti etici di un gruppo di esperti sull'intelligenza artificiale per un'IA affidabile:

a. Intervento e sorveglianza umani

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

b. Robustezza tecnica e sicurezza
c. Riservatezza e governance dei dati
d. Trasparenza
e. Diversità, non discriminazione ed equità
f. Benessere sociale e ambientale
g. Accountability

Successivamente il 19 febbraio 2020 la Commissione ha pubblicato il **Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia** con l'intento da un lato di promuovere l'adozione di un'IA affidabile e dall'altro lato di affrontare i rischi che possono derivare da questa tecnologia.[22] I libri bianchi sono documenti medianti i quali vengono formulate proposte di azione dell'UE in un determinato settore; il loro scopo principale è quello di avviare una discussione con il pubblico, le parti interessate, Il Parlamento europeo e il Consiglio. Nella parte introduttiva del libro bianco sull'IA vengono poste in evidenza le ragioni che hanno portato all'adozione del documento, analizzando in particolare il potenziale delle nuove tecnologie.[23] Viene così messo in risalto come l'IA cambierà le nostre vite migliorando l'assistenza sanitaria (garantendo diagnosi più precise e consentendo una migliore prevenzione delle malattie), migliorerà l'efficienza dei sistemi di produzione, aumenterà la sicurezza dei cittadini ed impatterà positivamente in altri molti casi che possiamo solo immaginare.[24] Al tempo stesso però vengono messi in luce alcuni aspetti che possono comportare una serie di rischi per gli individui, come ad esempio meccanismi decisionali non del tutto trasparenti, discriminazioni basate sul genere o di altro tipo, intrusioni nelle nostre vite

[22] Cfr. Moro P., Intelligenza artificiale e tecnodiritto. Fondamenti etici ed innovazione legislativa, in Moro P. (a cura di), Etica, Diritto e Tecnologia. Percorsi dell'informatica giuridica contemporanea, Franco angeli, Milano 2021, pp. 7-24 (p.17-18)
[23] Proietti G. "*Il libro bianco sull'intelligenza artificiale. L'approccio europeo tra diritto ed etica*" Giustiziacivile.com n. 6/2020
[24] Libro Bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia - Bruxelles, 19.2.2020 COM(2020) 65 final

private o utilizzi per scopi criminali. Ecco che allora data la centralità che l'IA ricopre e ricoprirà sempre di più nel corso dei prossimi anni per gli esseri umani, l'affidabilità di tale tecnologia risulta essere non solo un requisito fondamentale ma anche un prerequisito per la diffusione dell'IA; è infatti necessario che essa si sviluppi nel rispetto dei valori europei e dei diritti fondamentali come la dignità umana e la privacy.

Coerentemente alla linea programmatica precedentemente delineata si sottolinea poi la necessità di sviluppare un ecosistema di intelligenza artificiale comune che porti benefici all'intera società ed economia europea, evitando dunque la frammentazione del mercato unico poiché le singole iniziative nazionali minerebbero la certezza del diritto e indebolirebbero la fiducia dei cittadini nei confronti delle nuove tecnologie.

Altra riflessione operata dalla Commissione europea concerne la valutazione dell'idoneità della vigente disciplina giuridica alla luce delle nuove tecnologie emergenti. Sotto questo profilo viene messo in evidenza come alcune discipline vigenti siano applicabili ai sistemi di IA; viene fatta così menzione della normativa sulla protezione dei dati personali e la non discriminazione, oppure della legislazione riguardante la tutela dei consumatori. Tuttavia, alcune caratteristiche di questa tecnologia possono rendere più difficile l'applicazione della normativa vigente e proprio per questi motivi la Commissione ritiene che il quadro normativo europeo possa essere migliorato per meglio adattarsi alle nuove sfide che l'IA propone.

Proprio in questa direzione si muovono anche i successivi interventi normativi dell'UE; così nelle conclusioni del 21 ottobre 2020 (La *Carta dei diritti fondamentali nel contesto dell'intelligenza artificiale e della trasformazione digitale*) il Consiglio dell'Unione Europea ha esortato ad affrontare l'opacità, la complessità, l'imprevedibilità e l'autonomia di determinati sistemi di IA, al fine di garantire la loro compatibilità con i diritti fondamentali dell'UE.

Il 20 ottobre 2020, il Parlamento Europeo ha adottato varie risoluzioni relative all'intelligenza artificiale e la robotica, per quanto riguarda in particolare gli aspetti etici, la responsabilità civile e i diritti d'autore.

Il 9 marzo 2021 la Commissione ha presentato la visione e le prospettive per la trasformazione digitale dell'Europa entro il 2030 al fine di assicurare uno sviluppo dell'IA secondo modalità che rispettino i diritti delle persone e che rendano l'Europa pronta ad operare nell'era digitale.

Infine, il 21 aprile 2021 è stata presentata la proposta di regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'IA. Su tale proposta ci si soffermerà dettagliatamente nel corso della trattazione, intanto, per far comprendere l'importanza di tale proposta, si evidenzia il fatto che il c.d. IA ACT (come viene definita tale proposta) viene oggi visto come la legge europea sull'intelligenza artificiale. Assume poi ulteriore importanza poiché il regolamento è un atto legislativo di portata generale obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli stati membri (*art. 298 del Trattato sul Funzionamento dell'Unione Europea*).[25]

2. LA DEFINIZIONE DI INTELLIGENZA ARTIFICIALE

Come sottolineato nella parte introduttiva di questo elaborato il termine "*intelligenza artificiale*" venne coniato negli anni Cinquanta del XX secolo dallo scienziato John McCarthy; da ciò si ricava dunque che la terminologia non è certamente nuova, ma ha semplicemente avuto una diffusione sempre maggiore con il passare del tempo diffondendosi sia nel linguaggio comune che tra le varie discipline scientifiche, sociali e morali a causa dello

[25] Cfr. Moro P., Intelligenza artificiale e tecnodiritto. Fondamenti etici ed innovazione legislativa, in Moro P. (a cura di), Etica, Diritto e Tecnologia. Percorsi dell'informatica giuridica contemporanea, Franco angeli, Milano 2021, pp. 7-24 (p.18)

sviluppo esponenziale che le tecnologie digitali hanno avuto nell'epoca contemporanea.[26] La coniazione di un nuovo termine però, indipendentemente dall'ambito dove esso si inserisce, necessita molto spesso anche di una definizione che garantisca una maggiore certezza su cosa si intenda effettivamente rappresentare con quella determinata espressione. Ecco che dunque anche per il termine IA si è avvertita la necessita sin dalla sua nascita, di cercare di trovare una definizione che sia sufficientemente esaustiva per poter descrivere un fenomeno così complesso e in costante evoluzione.

Un punto di partenza per provare a definire un'IA è vedere come i dizionari moderni definiscono tale tecnologia, analizzando le eventuali differenze ed uguaglianze che possono sussistere.

Ecco che dunque l'*Enciclopedia on-line Treccani* definisce l'intelligenza artificiale (IA) la "*Disciplina che studia se e in che modo si possano riprodurre i processi mentali più complessi mediante l'uso di un computer. Tale ricerca si sviluppa secondo due percorsi complementari: da un lato l'i. artificiale cerca di avvicinare il funzionamento dei computer alle capacità dell'intelligenza umana, dall'altro usa le simulazioni informatiche per fare ipotesi sui meccanismi utilizzati dalla mente umana*."[27]

Il *Cambridge dictionary* offre la seguente definizione di IA: "*the study of how to produce machines that have some of the qualities that the human mind has, such as the ability to understand language, recognize pictures, solve problems, and learn*."[28]

[26] Cfr. Moro P., Intelligenza artificiale e tecnodiritto. Fondamenti etici ed innovazione legislativa, in Moro P. (a cura di), Etica, Diritto e Tecnologia. Percorsi dell'informatica giuridica contemporanea, Franco angeli, Milano 2021, pp. 7-24 (p.7)

[27] Enciclopedia Treccani definizione "intelligenza artificiale"; intelligènza artificiale nell'Enciclopedia Treccani
[28] Dictionary.cambridge.org/it/, s.v., "artificial intelligence", disponibile presso ARTIFICIAL INTELLIGENCE definizione, significato - che cosa è ARTIFICIAL INTELLIGENCE nel dizionario Inglese - Cambridge Dictionary

Entrambe queste definizioni fanno riferimento alla capacità dell'IA di creare delle macchine che siano in grado di replicare i processi mentali umani o almeno una parte di essi e sotto questo punto di vista il collegamento fatto tra IA e mente umana risulta essere una costante anche in altre definizioni mediante le quali si è cercato di definire l'intelligenza artificiale. Lo stesso John McCarthy in un'intervista del 2007 per l'Università di Stanford alla domanda se fosse possibile definire una qualsiasi forma di intelligenza in generale senza necessariamente relazionarla all'intelligenza umana rispose "N*ot yet"*[29] sottolineando così ulteriormente il bisogno umano di confrontare anche le nuove tecnologie con il proprio intelletto. Anche la definizione di IA da un punto di vista della scienza informatica presenta una connessione con l'intelligenza umana; infatti una delle definizione più accreditate in tale ambito, riconosciuta anche a livello internazionale, è quella che definisce l'intelligenza artificiale come "*una disciplina che studia i fenomeni teorici, le metodologie e le tecniche che permettono di progettare sistemi hardware e sistemi di programmi software capaci di fornire all'elaboratore elettronico delle prestazioni che, a un osservatore comune, sembrerebbero essere di pertinenza esclusiva dell'intelligenza umana"*[30]

Da un punto di vista legislativo l'Unione Europea nel cercare di creare un framework giuridico per l'IA ha sempre incentivato le varie istituzioni dell'Unione stessa a fornire una definizione di IA più chiara e precisa possibile; così per esempio nell'allegato alla risoluzione del Parlamento europeo del 16 febbraio 2016 viene stabilito che: " *È opportuno stabilire una definizione comune europea di robot autonomo intelligente, comprese eventualmente le definizioni delle sue sottocategorie, tenendo conto delle seguenti caratteristiche:*

[29] McCathy J.; "*What is Artificial Intelligence*", 2007, reperibile in: http://www-formal.stanford.edu/jmc/whatisai.pdf
[30] Somalvico M.; "*L'intelligenza Artificiale*", Rusconi, Milano, 1987

- *la capacità di acquisire autonomia grazie a sensori e/o mediante lo scambio di dati con il proprio ambiente (interconnettività) e l'analisi di tali dati;*
- *la capacità di apprendimento attraverso l'esperienza e l'interazione;*
- *la forma del supporto fisico del robot;*
- *la capacità di adeguare il suo comportamento e le sue azioni all'ambiente."*[31]

Successivamente nell'allegato della *Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale* all'art. 3 viene stabilito che ai fini di questo regolamento si intende per sistema di intelligenza artificiale (IA): "*un sistema basato su software o integrato in dispositivi hardware che mostra un comportamento che simula l'intelligenza, tra l'altro raccogliendo e trattando dati, analizzando e interpretando il proprio ambiente e intraprendendo azioni, con un certo grado di autonomia, per raggiungere obiettivi specifici."*[32]

L'*AI Act* a sua volta fornisce una definizione ancora diversa: "*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.*" [33]

Quest'ultima tra tutte le definizioni che si sono provate a dare di IA è forse quella più generica e aperta; ciò non è assolutamente casuale ma si è volontariamente scelto di dare una definizione così ampia in modo tale da poter far rientrare in essa anche eventuali future tecnologie senza dover creare nuove definizioni all'ormai inarrestabile avanzare tecnologico.

[31] Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL))
[32] Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL))
[33] Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzare sull'intelligenza artificiale (Legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione

Come si nota dunque, la ricerca di una definizione univoca e omnicomprensiva di tutti gli aspetti e peculiarità dell'IA risulta piuttosto complessa poiché cercare di imbrigliare in poche parole qualcosa di così sofisticato e mutevole non solo è complicato da compiere ma può risultare anche dannoso per lo sviluppo futuro della tecnologia stessa. Ecco quindi che allo stato attuale delle cose una definizione così ampia come quella fornita dall'*IA Act* sembra essere un compromesso più che accettabile.

3. CONCETTI FONDAMENTALI NELL'IA: DEFINIZIONI CHIAVE

Come evidenziato poco sopra la definizione di IA non risulta così semplice, anche perché all'interno dell'espressione intelligenza artificiale si fanno ricadere nozioni, concetti e tecnologie che hanno un utilizzo, una funzione e un significato diverso tra loro. Proprio per questo motivo, anche al fine di comprendere meglio determinati concetti che riaffioreranno nel corso di tale tesi, è bene fin da subito cercare di dare una definizione di alcune fondamentali nozioni legate al mondo dell'intelligenza artificiale.

A) MACHINE LEARNING

Nel 1959 il concetto di machine learning fu introdotto per la prima volta da Arthur Lee Samuel, un rinomato ricercatore statunitense nel campo dell'intelligenza artificiale. Tuttavia, è a un altro illustre scienziato americano, Tom Michael Mitchell, che dobbiamo la definizione più iconica di machine learning: "*Si dice che un programma apprende dall'esperienza E, con riferimento ad alcune classi di compiti T e con misurazione della performance P, se le sue performance nel compito T, come misurato da P, migliorano con l'esperienza E*."[34] Per spiegarlo in modo

[34] Mitchell T. M.; "*Machine Learnin*g", McGraw-Hill 1997

più semplice, attraverso l'esperienza e il tempo la macchina migliora progressivamente le sue risposte alle situazioni reali che affronta di volta in volta.

Il Machine Learning (detto anche ML) oggi possiamo considerarlo come il cuore pulsante dell'IA, in quanto permette di rompere con l'approccio tradizionale e introduce un concetto più avanzato: l'apprendimento attraverso i dati. Sostanzialmente, dunque, una macchina invece di essere programmata per eseguire azioni specifiche viene addestrata su un vasto corpus di dati in modo da imparare e migliorare autonomamente nel tempo. Questo processo di apprendimento è orchestrato dall'identificazione di modelli nei dati; infatti, gli algoritmi di ML operano cercando di cogliere regolarità e tendenze all'interno dei dati forniti. A mano a mano che la macchina acquisisce sempre più dati, si adatta, raffinandosi nell'elaborazione di informazioni complesse e nella risoluzione di problemi.[35]

Il ML costituisce un vasto territorio all'interno del quale incontriamo tipologie e approcci distinti che costituiscono un panorama estremamente ricco e sfaccettato che riflette la complessità delle sfide affrontate dall'intelligenza artificiale; tra queste diverse tipologie le principali sono:

- **Supervised Learning:** Questa categoria del machine learning rappresenta una delle fondamenta su cui poggia l'automazione intelligente. Qui, i modelli vengono addestrati utilizzando un insieme di dati precedentemente etichettati. Questi dati contengono risposte note e l'obiettivo del modello è apprendere a mappare correttamente gli input alle risposte corrispondenti. Dopo l'addestramento, il modello è in grado di fare previsioni su nuovi dati simili, determinando quali risposte potrebbero corrispondere a determinati input. Un esempio concreto è l'addestramento di un modello per il

[35] Sanguinetti G.; "*Machine Learning: accuratezza, interpretabilità e incertezza*" Ithaca: Viaggio nella Scienza XVI, 2020 • Machine Learning Uncertainty, p. 78

riconoscimento di immagini di gatti e cani, dove le immagini sono etichettate come "*gatto*" o "*cane*".

- **Unsupervised Learning:** In contrasto al supervised learning, l'unsupervised learning coinvolge dati non etichettati, il che significa che mancano risposte o etichette. Qui, i modelli cercano di scoprire pattern nascosti o strutture all'interno dei dati. L'obiettivo principale è comprendere la struttura dei dati stessi, senza alcuna guida predefinita. Una delle applicazioni più comuni è la clusterizzazione,[36] dove il modello raggruppa dati simili in cluster omogenei. Ad esempio, questa tecnica potrebbe essere usata per segmentare clienti in gruppi simili per una strategia di marketing mirata.
- **Reinforcement Learning:** Questo paradigma di apprendimento è ispirato al comportamento degli organismi biologici che apprendono attraverso l'interazione con l'ambiente. I modelli di reinforcement learning apprendono a prendere decisioni basate su una serie di azioni e feedback dall'ambiente. Questo è ampiamente utilizzato nell'addestramento di agenti virtuali come robot o intelligenze artificiali per videogiochi, per imparare a prendere decisioni ottimali in un ambiente dinamico e incerto.
- **Deep Learning:** Nel contesto del machine learning, il deep learning rappresenta una frontiera avanzata. Questa sottocategoria coinvolge reti neurali artificiali profonde,[37] ispirate al funzionamento delle reti neurali nel cervello umano. Grazie a livelli di neuroni interconnessi, queste reti sono particolarmente efficaci nell'analizzare dati complessi come immagini, suoni e testo. Il deep learning è all'origine di notevoli

[36] Cfr. dizionario Treccani: nel linguaggio scient. e tecn., insieme di oggetti collegati tra loro; metodo per individuare in una popolazione caratteristiche che presentino un certo livello di correlazione

[37] Cfr. Ali Alessio Salman "*Reti neurali artificiali: dal MLP alle più recenti architetture di Convolutional Neural Networks*" (2017); Una rete neurale artificiale è un modello di calcolo ispirato ai principi di funzionamento del sistema nervoso degli organismi evoluti. La caratteristica fondamentale di una rete neurale è che essa è capace di acquisire conoscenza modificando la propria struttura in base alle informazioni esterne (i dati in ingresso) e interne (le connessioni) durante il processo di apprendimento.

avanzamenti, come il riconoscimento di oggetti nelle immagini e la traduzione automatica. Le reti neurali profonde sono composte da numerosi strati, consentendo loro di catturare progressivamente dettagli sempre più fini dai dati, creando rappresentazioni sempre più sofisticate. [38]

In conclusione, il machine learning si configura come un'infrastruttura vitale per l'evoluzione dell'intelligenza artificiale. La capacità di apprendere dai dati e adattarsi alle nuove sfide pone le basi per innovazioni sempre più avanzate in campi come la medicina, l'automazione industriale e molte altre.

B) BIG DATA

Una definizione analiticamente precisa di "*Big Data*" è ardua, dato che l'espressione stessa fa riferimento ad una "*grandezza*" indeterminata e il concetto di "*dato*" non è oggettivo, in quanto dipende dalla prospettiva dell'osservatore e dall'identificazione del suo significato.[39] Sono dunque in molti ad avere cercato di dare una definizione; la più condivisa caratterizza i Big Data in termini di quattro variabili (le 4 V dei Big Data):

- *Volume (dimensioni)*
- *Varietà*
- *Velocità*
- *Veridicità (o affidabilità)*

Almeno in apparenza, uno dei parametri più evidenti è rappresentato dal ***volume*** dei dati stessi. Quando la quantità di informazioni supera una certa soglia (seppur arbitraria), le tradizionali metodologie di analisi, che implicano l'intervento umano, diventano impraticabili. Qui entra in

[38] Buyers J.; "*Artificial Intelligence. The pratical legal issues*", Londra, 2018, p. 43
[39] Ferrari V.; Note socio-giuridiche introduttive per una discussione su diritto, intelligenza artificiale e big data 24 Novembre 2020

gioco il machine learning, ad esempio, e altre tecniche che consentono alle macchine di apprendere autonomamente. In modo analogo, quando la ***varietà*** dei dati o la loro complessità supera un determinato limite, nuovamente l'analisi convenzionale diviene un'impresa irrealizzabile. La ***velocità*** di generazione dati è strettamente collegata al problema del volume: se una rete produce informazioni a una velocità troppo elevata per l'elaborazione umana, è necessario adottare tecniche alternative. Fondamentalmente, tutte queste caratteristiche condividono un tratto comune: il concetto di Big Data. Questo termine viene applicato quando il potenziale computazionale necessario per estrarre significato da tali dati diventa insostenibile con le tradizionali metodologie, rendendo necessario un approccio basato su tecniche automatiche che riescano ad emulare alcune delle abilità umane. Per quanto riguarda la questione della ***veridicità*** dei dati essa è trasversale e non si limita esclusivamente ai Big Data. Spesso, infatti, i dati si presentano incompleti, imprecisi e talvolta persino errati. Ecco che questa mancanza di completezza diventa sempre più difficile da gestire all'aumentare del volume e della complessità dei dati, con conseguenze inevitabili sull'accuratezza dei risultati ottenuti. Piuttosto che essere una caratteristica distintiva, la veridicità dei dati deve essere considerata come un fattore limitante che influenza i Big Data in generale.[40]

Nonostante l'incertezza dal punto di vista della definizione di Big Data, risulta innegabile che la rivoluzione originata dall'integrazione tra Intelligenza Artificiale e Big Data stia avanzando a passi da gigante, sia nell'ambito delle scienze naturali che in quello delle scienze sociali. L'accesso immediato a miliardi di dati, selezionabili in maniera rapida attraverso algoritmi complessi, consente di cogliere la portata globale di fenomeni tradizionalmente studiati in modo frammentario. In particolare, nelle scienze sociali, dove spesso ci si affida a campionamenti, questa tecnologia permette di concentrarsi all'interno di queste molteplici

[40] Longo G.; "*Big Data e intelligenza artificiale: che futuro ci aspetta?*" n. 20.2018, p. 101ss

informazioni su aspetti minoritari dei fenomeni stessi, considerandoli in connessione con l'insieme più ampio.[41] Ciò accade regolarmente in diversi campi, fra cui, quello commerciale, dove l'offerta di beni e servizi avviene sempre più in modo profilato, a partire dalla conoscenza delle preferenze manifestate dai singoli attraverso la navigazione in rete. Anche in settori economicamente volatili come quello borsistico, l'analisi di grandi quantità di dati facendo ricorso a learning machines è ben diffusa e con rimarchevoli risultati finanziari, potendo permettere previsioni altamente affidabili sugli sviluppi dei singoli mercati.[42]

In conclusione, in un'epoca in cui l'informazione è una risorsa essenziale, i Big Data emergono come una forza motrice che sta ridefinendo profondamente ogni aspetto delle nostre vite. Il loro impatto nell'era moderna è innegabile, dall'accelerazione dell'innovazione scientifica all'ottimizzazione dei processi aziendali. Con la capacità di rivelare pattern complessi, anticipare tendenze e guidare decisioni informate, i Big Data si pongono al centro dell'evoluzione tecnologica e sociale, aprendo nuovi orizzonti per l'intelligenza artificiale, la medicina, l'ambiente e molto altro. L'importanza di saper gestire e interpretare in modo etico questa straordinaria fonte di conoscenza è fondamentale per guidare il progresso e il benessere della società in un futuro sempre più interconnesso e guidato dai dati.

C) IA FORTE E IA DEBOLE

Nel contesto dell'intelligenza artificiale possiamo fare una distinzione tra "*IA forte*" e "*IA debole*". Entrambi tali sistemi in qualche modo riflettono, per così dire, due diverse direzioni di ricerca e sviluppo nell'ambito della simulazione della mente umana da parte dell'intelligenza artificiale.

[41] Mangiameli A.; "*Intelligenza artificiale, big data e nuovi diritti*"; Fascicolo 1-2022 Rivista Italiana di informatica e diritto, p. 75ss

[42] Ferrari V.; Note socio-giuridiche introduttive per una discussione su diritto, intelligenza artificiale e big data 24 Novembre 2020

Questa distinzione tra IA forte e IA debole viene tradizionalmente ricondotta a John Searle, il quale nel 1980 con la pubblicazione del libro "*Menti, cervelli e programmi"* definisce l'IA debole come uno strumento ausiliare alla mente umana, mentre l'IA forte al contrario non è un semplice simulatore della mente ma una vera e propria mente con relativi stati cognitivi annessi.[43] Da un lato dunque vengono individuati dei sistemi di intelligenza artificiale che sono sì in grado di superare la capacità della mente umana, ad esempio dal punto di vista della velocità e della precisione, ma che comunque rimangono ancorati al campo per il quale sono state predisposte (AI debole); dall'altro lato invece vengono individuati dei sistemi di intelligenza artificiale che sono in grado non solo di simulare un comportamento umano ma di svilupparne anche uno proprio, indipendentemente anche dal contesto di partenza all'interno del quale sono inseriti (AI forte).

Volendo meglio chiarire la distinzione tra intelligenza artificiale debole e forte la si potrebbe porre anche dal punto di vista dell'autonomia di tali sistemi. In questa prospettiva, si definisce IA debole quel sistema di programmi progettato per risolvere problemi specifici. In questo contesto, l'assistenza umana risulta sempre indispensabile poiché la macchina, non possedendo autonomia, non sarebbe in grado di compiere alcuna attività senza la supervisione umana. L'obiettivo di tali sistemi è quello di sostenere le attività umane in situazioni complesse, sviluppando un'imitazione di intelligenza su compiti specifici. Dall'altra parte, l'IA forte rappresenta un sistema che conferisce al calcolatore autonomia nei processi di pensiero, consentendogli di agire senza una necessaria supervisione umana.[44]

Come detto precedentemente IA forte e IA debole incarnano due approcci distinti nel mondo dell'intelligenza artificiale; mentre l'IA forte allo stato attuale sembra incarnare un'aspirazione ambiziosa di creare macchine che superino l'intelligenza umana in tutti gli aspetti, l'IA debole

[43] Searle John R.; "*Minds, Brains and Programs, in The Behavioral and Brain Sciences"*, 1980, Cambridge University Press

[44] Baroglio C.; "*L'Intelligenza Artificiale? È un gioco!"* atti del convegno dimatica 7-8 ottobre 2021, Palermo

riflette meglio lo stato attuale della nostra tecnologia, vale a dire sistemi artificiali estremamente specializzati che eccellono in compiti specifici ma che mancano di una vera comprensione e generale e autonoma.

CAPITOLO II - IL GDPR:

Come già evidenziato in parte nel capitolo precedente, lo sviluppo tecnologico è caratterizzato da una certa dicotomia circa l'impatto che esso possa avere nella nostra società. Se da un lato vengono sottolineati i benefici che molteplici settori possono trarre dal progresso tecnologico, dall'altro lato vengono messi sotto i riflettori i vari problemi e le varie preoccupazioni che sorgono e che possono sorgere, specie per quanto riguarda la tutela dell'individuo. Proprio quest'ultimo punto, la tutela dell'individuo, è stata ed è oggetto di forte attenzione da parte del legislatore europeo, attento sì a permettere e non limitare lo sviluppo di nuove tecnologie, ma allo stesso tempo a porre diritti come quello della privacy o della libertà individuale alla base delle legislazioni che si sono susseguite nel corso del tempo. Ecco che dunque in un mondo dove il singolo è sempre più relazionato con l'IA, non solo profittando dei suoi benefici, ma esponendosi anche ai suoi rischi, è bene cercare di capire, prima ancora di affrontare l'ultima novità legislativa introdotta in tema di IA dall'Unione europea, quali sono gli strumenti di difesa predisposti per lui dall'ordinamento europeo. In tale ambito, dal punto di vista legislativo, abbiamo una serie di interventi istituzionali susseguitesi nel corso del tempo che hanno cercato di regolamentare e armonizzare tra i vari stati dell'Unione la disciplina.

1. IL DIRITTO ALLA PRIVACY

A) La nascita del diritto alla privacy

Norberto Bobbio sosteneva che i diritti umani "*sono diritti storici, cioè nati in certe circostanze […] gradualmente, non tutti in una volta e non una volta per sempre.*"[45] Tale affermazione sembra calzare a pennello con la nascita del diritto alla privacy. La sua prima definizione risale alla fine del XIX secolo ed è dovuta non tanto ad una proposta di legge o ad una sentenza ma a ciò che oggi potremmo definire come vero e proprio gossip. Infatti ciò che spinse Samuel D. Warren a scrivere un articolo in difesa del diritto alla privacy, insieme al suo socio nonché futuro giudice della Corte Suprema, Louis D. Brandies, fu l'essere costantemente bersagliato dai giornali scandalistici a causa delle numerose infedeltà della moglie.[46] Ecco che allora il 15 dicembre 1890 pubblicarono un articolo che trattava il diritto alla privacy sulla rivista legale Harvard Law Review.[47] L'importante contributo di Warren e Brandeis fu la definizione della privacy come un diritto autonomo, distinto e indipendente da altri istituti legali che riguardavano la reputazione delle persone, come la calunnia e la diffamazione, o dai diritti di proprietà intellettuale, quali opere letterarie e artistiche. Il concetto di diritto alla privacy è efficacemente racchiuso nell'acclamata espressione "*the right to be let alone*", che si traduce come il "*diritto di essere lasciati in pace*". Questo diritto si configura quindi come un diritto "negativo" con radici tipicamente liberali, infatti per Warren e Brandies la privacy è un diritto da difendere e proteggere contro le invasioni esterne: la protezione statale non può interferire nella sfera interna del cittadino.[48]

B) Il diritto alla privacy nella Dichiarazione Universale dei Diritti Umani

Questa visione moderna del diritto, che mette al centro la persona e le proprie prerogative, è sopravvissuta nel corso del tempo ed è stata anche ripresa in alcuni trattati internazionali successivamente adottati. Nel 1947, in un periodo storico segnato da tensioni durante la Guerra

[45] Bobbio N.; "*L'età dei diritti*", Torino, 1990, p. 13-14
[46] Green M., Nørgaard L., Cyril B., Birkedal B.; "Early Modern Privacy: Sources and Approaches", MetteIntersections, 2022, p. 78-80
[47] Warren S. D., Brandies L. D.; "*Right to privacy*", in Harvard Law Review, 1980, p. 194-195
[48] Warren S. D., Brandies L. D.; "*Right to privacy*", in Harvard Law Review, 1980, p. 194-195

Fredda e dalla formazione di diversi schieramenti, le Nazioni Unite crearono un organismo composto da rappresentanti di otto Stati diversi. Questi membri furono selezionati dal Consiglio economico e sociale delle Nazioni Unite dando origine al Comitato per i Diritti Umani, il quale si è occupato di redigere un testo relativo ai diritti umani inalienabili.[49] Gli articoli difendono per la prima volta, il diritto alla vita, il riconoscimento alla propria personalità giuridica, l'uguaglianza davanti alla legge nonché quello che oggi si considera il diritto alla privacy.[50] Esso nasce nel 1948 con espresso riconoscimento nella Dichiarazione Universale dei Diritti Umani, approvata dall'Assemblea Generale delle Nazioni Unite il 10 dicembre;[51] all'articolo 12 della Carta viene sancito che: "*Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni.*"[52]

La Carta così riconosce espressamente un diritto negativo, configurandosi quest'ultimo come un'astensione dall'interferenza nella vita privata del singolo, adottando una visione che ben si concilia con quanto predisposto da Warren e Brandeis nel loro articolo.

C) Il diritto alla privacy nella Convenzione Europea dei Diritti dell'Uomo

La Convenzione Europea sui Diritti dell'Uomo fu firmata il 4 novembre 1950 a Roma; con 47 stati firmatari è entrata in vigore il 3 settembre 1953 ereditando i principi internazionali della Dichiarazione Universale dei Diritti Umani. È composta da 59 articoli divisi in 3 titoli.[53] Per quanto i riguarda il diritto alla privacy il riferimento è all'art. 8:

[49] Partipilo F., "*La Dichiarazione Universale dei Diritti Umani dal 1948 ai nostri giorni"*, Osservatoriodiritti, 2018
[50] Dichiarazione Universale dei Diritti Umani, Assemblea Generale Nazioni Unite, approvata il 10 dicembre 1948
[51] Soffientini M., Caccialupi M.; "*Privacy: protezione e trattamento dei dati*", PSOA Manuali, 2018, p. 53-55
[52] Dichiarazione Universale dei Diritti Umani, Assemblea Generale Nazioni Unite, approvata il 10 dicembre 1948.
[53] Moretti S.; "*La Convenzione Europea dei Diritti dell'Uomo compie 70 anni*" Questione di Giustizia, 2020

"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.*"

La stessa CEDU (Corte Europea dei Diritti dell'Uomo) ha definito il campo di applicazione dell'Articolo 8, sottolineando, tuttavia, che esso non è privo di limiti. La Convenzione impone un obbligo simultaneamente negativo e positivo, il che significa che gli Stati devono astenersi dall'ingerire arbitrariamente nella vita privata dei singoli e, allo stesso tempo, devono agire in modo attivo per garantire che il diritto enunciato non venga violato nemmeno nelle relazioni interpersonali, ossia nei rapporti tra individui privati.[54] Tuttavia, l'ingerenza da parte delle autorità pubbliche non è sempre vietata, poiché l'ambito di applicazione della normativa rimane in parte indefinito e prevede alcune eccezioni. Nel secondo paragrafo dell'articolo in questione, vengono specificate le eccezioni all'obbligo negativo, tra cui la previsione di legge, la tutela della sicurezza nazionale, della pubblica sicurezza, del benessere economico del paese, la difesa dell'ordine pubblico, la prevenzione dei reati, la protezione della salute o della morale, nonché la protezione dei diritti e delle libertà altrui. Ciò implica che in queste situazioni lo Stato è autorizzato a intervenire nella sfera privata dei cittadini senza che ciò costituisca una violazione del diritto alla privacy. Tuttavia, è importante sottolineare che la semplice esistenza di una di queste minacce non è sufficiente per legittimare l'ingerenza; il giudizio sulla necessità dell'intervento dipenderà dalla discrezionalità di ciascuno Stato, che valuterà di caso in caso

[54] Dichiarazione Universale dei Diritti Umani, Assemblea Generale Nazioni Unite, approvata il 10 dicembre 1948

l'importanza dei valori fondamentali in gioco, cercando di bilanciare attentamente gli interessi in causa.[55]

2. LA LEGISLAZIONE COMUNITARIA IN RELAZIONE ALLA PROTEZIONE DEI DATI PERSONALI: Verso il GDPR

A) La Direttiva 95/46/CE

Un'ulteriore tappa fondamentale all'interno del panorama europeo, da un punto legislativo, in materia di protezione dei dati personali è certamente l'emanazione del c.d. *Data Protecion Directive* con la a Direttiva 95/46/CE. Tale Direttiva entrò in vigore nel 1995 ed era diretta a tutti gli Stati membri, i quali dovettero adottare una disciplina interna conforme ad essa entro il 31 dicembre 1996.[56]

Con la sua emanazione l'Unione Europea si pose l'obbiettivo di armonizzare le norme in materia di protezione dei dati personali per garantire un "flusso libero" (free flow of data) dei dati e promuovere un elevato livello di tutela dei diritti fondamentali dei cittadini effettuando un bilanciamento d'interessi sul piano sovranazionale e così regolamentando una disciplina che assicurasse un equilibrio tra la privatezza dei singoli ed il diritto dei Paesi membri al libero scambio di dati, anche personali. Molte delle disposizioni introdotte da questa direttiva continuano a essere rilevanti ancora oggi. In particolare, il ruolo del consenso e delle informative rappresenta ancora una pietra angolare nel trattamento dei dati personali. Un aspetto particolarmente interessante riguarda la relazione che la Direttiva aveva con i paesi al di fuori dello Spazio Economico Europeo; infatti essa proibiva il trasferimento di dati personali

[55] Stoddart J., Chan B., Joly Y., "*The European Union's Adequacy Approach to Privacy and International Data Sharing*" edited by Rothstein M., A; Knoppers B.M., The Journal of law, medicine & ethics, 03/2016, Volume 44, Fascicolo 1

[56] In Italia venne recepita con la legge 675/96 proprio nell'ultimo giorno utile, il 31 dicembre 1996

in paesi in cui non fosse garantito un livello adeguato di protezione in conformità alle disposizioni della direttiva stessa.[57]

Nonostante le indubbie virtù della direttiva, divenne presto evidente che essa stava diventando obsoleta, in gran parte a causa della rapidità con cui si stavano sviluppando le nuove tecnologie e cambiando il panorama della gestione dei dati personali. Era necessario dunque un quadro normativo più dinamico ed efficace per affrontare le sfide crescenti legate alla privacy e alla protezione dei dati. Ecco che quindi negli anni successivi la Direttiva fu progressivamente integrata e poi sostituita da nuovi regolamenti. Il regolamento CE n. 45/2001 rappresentò un passo importante nell'aggiornamento delle normative sulla protezione dei dati, mentre il regolamento UE 2016/679, noto come Regolamento Generale sulla Protezione dei Dati (GDPR), segnò un punto di svolta significativo abrogando la Direttiva 95/46/CE.

B) Il regolamento CE 45/2001 sulla protezione dei dati

Mentre i vari Stati membri dell'Unione Europea procedevano con l'attuazione graduale della direttiva 94/46/CE, l'UE intraprese un ulteriore passo fondamentale verso l'unificazione delle norme relative al trattamento dei dati personali da parte delle diverse istituzioni europee. Questo significativo avanzamento mirava a creare un quadro normativo coeso e armonizzato per l'intera Unione Europea, affrontando le sfide poste dalla gestione dei dati personali in un contesto sempre più digitalizzato e interconnesso. In ossequio a ciò è stato adottato il Regolamento n. 45/2001[58] che istituisce l'organo di controllo indipendente e detta le disposizioni necessarie per adeguare le norme di diritto derivato esistenti in materia.[59]

[57] Tosi E., Soro A., Franceschelli V., "*Privacy digitale: riservatezza e protezione dei dati personali tra GDPR e nuovo Codice privacy*", DNT Milano, Italy, 2019, p. 15ss
[58] Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati, Gazzetta ufficiale del 12/01/2001
[59] Faro S.; Informatica e diritto, XXX annata, Vol. XIII, 2004, n. 1-2, pp 14-15

L'introduzione di tale regolamentazione da parte dell'Unione Europea ha avuto un impatto significativo nel sottolineare l'importanza del diritto alla privacy. Tuttavia, una delle innovazioni più rilevanti è stata la creazione di una nuova figura, ossia il Garante Europeo della protezione dei dati, comunemente noto con l'acronimo inglese EDPS (*European Data Protection Supervisor*). Questa figura ha assunto un ruolo chiave nell'assicurare la tutela dei dati personali all'interno dell'Unione Europea, garantendo il rispetto delle normative sulla privacy e promuovendo una cultura di responsabilità nella gestione dei dati. Il Garante ha il compito di supervisionare e garantire l'applicazione delle disposizioni del regolamento e di qualsiasi altro atto comunitario relativo alla protezione delle persone fisiche in merito al trattamento dei dati personali. Questa sorveglianza si applica a tutte le istituzioni o gli organismi comunitari, ad eccezione della Corte di giustizia nell'esercizio delle sue funzioni giurisdizionali. Per quanto riguarda la Corte di giustizia, il controllo del Garante riguarda esclusivamente l'attività amministrativa, in particolare in relazione al personale della Corte. Inoltre, il Garante fornisce pareri su questioni relative al trattamento dei dati personali sia alle istituzioni e agli organismi comunitari che alle parti interessate.[60]

La Direttiva CE 45/2001 rappresentò dunque un passo significativo nell'ambito della protezione dei dati personali nell'Unione Europea. Essa introdusse norme e principi fondamentali, delineando il quadro per il trattamento dei dati personali all'interno delle istituzioni comunitarie. Tuttavia, col passare del tempo, divenne evidente che la direttiva era diventata obsoleta, incapace di affrontare le sfide poste dalle nuove tecnologie e i cambiamenti nel panorama della protezione dei dati necessitando di essere sostituita da normative più moderne e robuste come il GDPR, che si sono adattate meglio alle esigenze di un mondo digitalizzato e interconnesso.

[60] Iaselli M.; "*Sanzioni e responsabilità in ambito GDPR*", Compliance, 2019

3. IL GDPR

Il Regolamento del Parlamento Europeo del 27 aprile 2016, noto come GDPR (*General Data Protection Regulation*) è diventato operativo il 24 maggio 2016 e ha iniziato ad essere applicato a partire dal 25 maggio 2018. Questo significativo passo normativo ha portato all'abrogazione della precedente Direttiva UE 95/46/CE, nonché di tutte le leggi nazionali sulla protezione della privacy adottate dai singoli Stati Membri.[61] Il GDPR ha introdotto così un quadro legislativo più moderno e uniforme per la protezione dei dati personali nell'Unione Europea, mirando a garantire una maggiore coerenza e sicurezza nel trattamento dei dati in tutta l'UE.[62] In particolare l'approccio del nuovo regolamento è volto a responsabilizzare i titolari del trattamento affinché siano questi a individuare le misure più idonee per tutelare i soggetti interessati, sulla base di principi individuati dal regolamento stesso,[63] il quale è orientato a imporre come standard predefinito quello della massima protezione del soggetto interessato. Il nuovo regolamento porta con sé una serie di importanti innovazioni, che spaziano dall'introduzione di nuove figure istituzionali alla ridefinizione di concetti fondamentali come quello di "*dato personale*" e "*trattamento*". Queste modifiche sono finalizzate a includere una gamma più ampia di situazioni che possono rientrare nell'ambito di applicazione del regolamento. In sintesi, il nuovo regolamento ha ampliato notevolmente la sua portata per adattarsi alle sfide poste dalla crescente complessità del trattamento dei dati personali nell'era digitale.[64]

---

[61] Denley, A., Foulsham M., Hitchen B., "*GDPR: how to achieve and maintain compliance*", 2019, p 74-75
[62] Krzysztofek M., "*GDPR: Post-Reform Personal Data Protection in the European Union*", 2018, p.18
[63] I principi di liceità, correttezza, e trasparenza, individuati nell'art. 5 del regolamento
[64] Di Ciollo G.; *L'ambito di applicazione della normativa privacy: analisi comparata tra GDPR e direttiva 95/46/CE*, Iusinitinere, 2019

A) Oggetto e finalità

L'art 1 del GDPR[65] dichiara il duplice oggetto del Regolamento: la protezione delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione dei medesimi dati. Da ciò si evince che i due ambiti di regolamentazione sono pari ordinati senza che l'uno possa considerarsi prevalente sull'altro. Tale natura ambivalente delle disposizioni contenute nel Regolamento è in linea con l'originaria impostazione della dir. 95/46/CE relativa anch'essa alla "*tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati*" ed è frutto della maturata consapevolezza del legislatore europeo circa l'importanza di una tutela a 360 gradi dei dati personali.[66]

Con riferimento alla nozione "*protezione dei dati personali*" ci si riferisce alla necessità di garantire che le informazioni che identificano o possono identificare una persona fisica siano trattate in modo adeguato e sicuro. La protezione dei dati personali comprende una serie di principi fondamentali, tra cui possiamo citare:

- **Trasparenza:** Le persone devono essere informate su come vengono raccolti e utilizzati i loro dati personali.
- **Finalità legittime:** I dati personali possono essere raccolti solo per scopi specifici, chiari e legittimi.

[65] Cfr. Art. 1 GDPR : "*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*."

[66] Riccio G. M.; "*Gdpr e normativa privacy*" a cura di Riccio G. M.; Scorza G.; Belisario E.; "*Gdpr e normativa privacy*", Milano, IPSOA, 2018, p. 4-9

- **Minimizzazione dei dati:** Le organizzazioni devono raccogliere solo i dati necessari per scopi specifici e limitati.
- **Accuratezza:** I dati devono essere accurati e, se necessario, aggiornati.
- **Limitazione della conservazione:** I dati personali possono essere conservati solo per il tempo necessario al raggiungimento degli scopi per cui sono stati raccolti.
- **Integrità e riservatezza:** Deve essere garantita la sicurezza dei dati per prevenire perdite, danni o accessi non autorizzati. [67]

Per "*libera circolazione dei dati*" invece possiamo ritenere che questo concetto si riferisce alla possibilità di trasferire dati personali tra paesi dell'Unione Europea senza restrizioni ingiustificate. Il GDPR promuove la libera circolazione dei dati all'interno dell'UE per sostenere il mercato unico digitale. Ciò significa che le organizzazioni possono trasferire dati tra Paesi Membri senza la necessità di ulteriori autorizzazioni o misure di sicurezza, purché rispettino le disposizioni del regolamento in materia di protezione dei dati personali.

La libera circolazione dei dati è essenziale per consentire alle imprese di operare senza ostacoli all'interno del mercato unico europeo e per garantire che i cittadini europei possano usufruire dei servizi digitali in modo agevole, indipendentemente dal paese in cui risiedono. Tuttavia, questa circolazione deve avvenire nel rispetto delle norme di protezione dei dati personali stabilite dal GDPR, garantendo che i diritti e le libertà delle persone siano tutelati in tutti i contesti.[68]

Per quanto riguarda invece le finalità del Regolamento anche qui, come nel caso dell'oggetto, ne vengono individuate due; stabilire che, in Europa, "*la protezione delle persone fisiche con*

[67] Zorzi Galgano N.;. "*Persona E Mercato Dei Dati. Riflessioni Sul" GDPR*. CEDAM, 2019, p 35-42

[68] Maglio, M.; "*Manuale di diritto alla protezione dei dati personali – La privacy dopo il regolamento UE".* Milano, Maggioli Editore, 2017, p. 43

riguardo al trattamento dei dati di carattere personale è un diritto fondamentale"[69] e "*contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche*".[70] In questa prospettiva il Regolamento persegue lo scopo di creare sempre più uniformità della disciplina europea in tale materia sottolineando come l'attuale contesto socio-economico e tecnologico "*richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno*".[71]

Il Regolamento è volto così a porre rimedio sia alla poca uniformità nella disciplina dei singoli Stati Membri sia ad accrescere il livello di certezza del diritto e fiducia dei cittadini europei nell'effettiva protezione dei propri dati personali. Ciò viene garantito anche dal fatto che la disciplina introdotta con il GDPR è costruita attorno ad una serie di istituti che presentano un pragmatismo e un'operatività decisamente superiore alla disciplina precedente; il Regolamento infatti predispone adempimenti di carattere più pregnante, capaci per un verso di responsabilizzare maggiormente i titolari dei trattamenti e, per altro verso, di garantire agli interessati una consapevolezza effettiva in relazione ai trattamenti posti in essere nei confronti dei propri dati personali e ai propri diritti connessi a tali trattamenti.[72]

La ricerca di uniformità tra i vari Stati Membri non impedisce comunque una certa discrezionalità in certi ambiti da parte di questi ultimi;[73] la stessa scelta di optare per un Regolamento e non una Direttiva, lasciando dunque un certo margine decisionale ai vari Stati,

[69] Cfr. Considerando 1 GDPR
[70] Cfr. Considerando 2 GDPR
[71] Cfr. Considerando 7 GDPR
[72] Riccio G. M.; "*Gdpr e normativa privacy*" a cura di Riccio G. M.; Scorza G.; Belisario E.; "*Gdpr e normativa privacy*", Milano, IPSOA, 2018, p. 4-9
[73] Cfr. Considerando 10 GDPR

è sintomatica di questa visione, volendo anche evitare di creare una disciplina fin troppo rigida in un settore sempre più penetrato da sviluppi tecnologici che mutano rapidamente il contesto all'interno del quale la normativa deve operare.

B) L'ambito di applicazione materiale

Il paragrafo 1 dell'articolo 2 del regolamento definisce chiaramente il campo di applicazione materiale del GDPR, seguendo in gran parte la definizione fornita dall'articolo 3 della direttiva 95/46/CE.[74] Questo campo di applicazione riguarda sia il trattamento completamente o parzialmente automatizzato di dati personali, sia il trattamento non automatizzato di dati personali contenuti in un archivio o destinati ad esservi inseriti.

Ciò che differisce è la definizione stessa di "*dato personale*" contenuta nell'articolo 4 del regolamento. In questa nuova definizione, sono stati introdotti elementi identificativi aggiuntivi come "*il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online*"[75] mentre gli elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale figuravano già nella scorsa direttiva. Questi nuovi elementi ampliano la gamma di informazioni che possono essere considerate dati personali e includono dati relativi alla localizzazione di un individuo, così come pseudonimi virtuali e non, che possono essere ricondotti a una persona fisica o giuridica.[76] Ad esempio, i portafogli digitali delle criptovalute, noti come "wallet", rientrano in questa categoria, poiché anche se le stringhe alfanumeriche sono pubblicamente accessibili, possono essere ricondotte a un soggetto

[74] Cfr. Art. 3 paragrafo 1 Direttiva 95/46/CE
[75] Cfr. Art. 4 GDPR " «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
[76] Cfr. considerando 26 del GDPR: "I dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile"

specifico come un individuo o un'entità giuridica. Da ciò deriva che l'individuazione o la possibilità di individuare il soggetto cui si riferisce il dato pseudonimizzato è ora sufficiente per considerare l'informazione come un dato personale ai sensi del regolamento. I dati anonimi invece, come specificato anche nel considerando 26 del regolamento, non rientrano nell'ambito di applicazione delle sue disposizioni. [77]

La definizione di "*trattamento*" invece, come stabilita nel regolamento, copre una vasta gamma di diciassette attività relative ai dati personali. Queste attività iniziano con la fase di raccolta dei dati e terminano con la loro cancellazione o distruzione. In altre parole, il trattamento comprende qualsiasi utilizzo dei dati, che può essere sia positivo (ad esempio, l'elaborazione o l'analisi dei dati) sia negativo (come la cancellazione o la limitazione del loro utilizzo). In particolare, il regolamento riconosce come soggetto di interesse specifico alcune forme speciali di trattamento, tra cui la profilazione. Questa consiste nell'elaborazione automatica dei dati al fine di valutare aspetti personali di un individuo e creare un profilo basato su tali dati. La rilevanza di questo tipo di trattamento risiede principalmente nella sua intrusività a livello personale, poiché consente di prevedere le preferenze o il comportamento della persona interessata.[78] [79] Questo concetto è riflesso nel riconoscimento del diritto di un individuo "*a non essere soggetto a una decisione [...] basata unicamente su un trattamento automatizzato*."[80]

Il regolamento stabilisce un'eccezione al suo ambito di applicazione, nota come "*household exclusion provision*," che riguarda i trattamenti di dati personali effettuati nell'ambito di attività strettamente personali o domestiche. Questa disposizione solleva alcune questioni

[77] Terolli E.; Diritto dell'Informazione e dell'Informatica (Il), fasc.1, 1 febbraio 2021
[78] Cfr. Amidei A.; "*Robotica intelligente e responsabilità: profili e prospettive evolutive del quadro normativo europeo*", in Ugo Ruffolo, "*Intelligenza artificiale e responsabilità*", Giuffrè, 2017, pp. 63-70
[79] L'ipotesi di profilazione ai fini di somministrazione di pubblicità mirate è analizzata dal considerando 70
[80] Cfr. Art. 22 paragrafo 1 GDPR " 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."

interpretative poiché non è sempre chiaro quando un trattamento assume un carattere strettamente personale.

Il considerando 18 del regolamento fornisce alcune chiarezze in merito a questa disposizione citando alcune attività che rientrano in questa eccezione, come ad esempio l'uso dei social network, la corrispondenza o la gestione degli indirizzi personali.

Per determinare se un trattamento rientri nell'ambito personale e domestico, il Gruppo di lavoro istituito dall'articolo 29 della precedente direttiva (WP29)[81], ora sostituito dal Comitato europeo per la protezione dei dati (EDBP), ha sviluppato delle linee guida generali. Queste linee guida prendevano in considerazione diversi fattori, tra cui:

- La possibilità che i dati siano diffusi a un pubblico indeterminato.
- L'esistenza o meno di una relazione personale con i soggetti i cui dati sono trattati.
- L'assenza di connotati di professionalità o sistematicità nel trattamento.
- Il potenziale per un'illecita intrusione nella privacy dovuta al trattamento dei dati.

Sono altresì esclusi dall'applicazione del regolamento i trattamenti effettuati dalle autorità preposte alla tutela della pubblica sicurezza nell'esercizio delle loro funzioni, nonché gli uffici, agenzie, istituzione e organi dell'Unione, ai quali si applica invece il regolamento 2001/45/CE, e infine i trattamenti aventi ad oggetto dati di persone defunte. [82]

C) L'ambito di applicazione territoriale

Dal punto di vista dell'applicazione territoriale il GDPR ha avuto un importante impatto, e continua tuttora ad averlo, non solo nei confronti degli Stati Membri dell'UE, ma anche nei

[81] WP29, Proposals for Amendments regarding exemption for personal or household activities
[82] Terolli E.; Diritto dell'Informazione e dell'Informatica (Il), fasc.1, 1 Febbraio 2021

confronti di organizzazioni esterne all'Unione Europea stessa, le quali sono destinatarie di alcuni obblighi introdotti dalla normativa.

In merito a questo, diverse nazioni, tra cui ad esempio la Repubblica Popolare Cinese, il Regno di Thailandia e l'India, insieme ad altri paesi che finora non hanno fornito adeguati livelli di tutela per la protezione dei dati personali, sono state obbligate ad adeguarsi a una legislazione estremamente tecnica e dettagliata, come quella del GDPR. Questa iniziativa ha comportato l'integrazione di testi normativi nazionali, spesso carenti, al fine di garantire una maggiore protezione della privacy e la conformità alle norme internazionali sulla protezione dei dati.[83] Il GDPR adotta infatti una concezione di estensione territoriale più ampia sia rispetto al vecchio "*Codice in materia della protezione dei dati personali*" italiano,[84] ma anche rispetto alla già più volte citata Direttiva 95/46/CE.[85]

---

[83] Cfr. D'Anna A.; "*L'ambito di applicazione territoriale del regolamento generale per la protezione dei dati personali*", Horisma, 2019, p. 61-83 a cura di Bonavita S.; "*Società delle tecnologie esponenziali e general data protection regulation: la circolazione internazionale dei dati personali"*

[84] Cfr. Articolo 5 del Decreto Legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, (c.d. "Codice della privacy")

"Oggetto ed ambito di applicazione"

1. Il presente codice disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato.

2. Il presente codice si applica anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea. In caso di applicazione del presente codice, il titolare del trattamento designa un proprio rappresentante stabilito nel territorio dello Stato ai fini dell'applicazione della disciplina sul trattamento dei dati personali.

[85] Cfr. Articolo 4 della 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

"Campo di applicazione"

1. Le disposizioni della presente direttiva si applicano al trattamento di dati personali interamente o parzialmente automatizzato nonché al trattamento non automatizzato di dati personali contenuti o destinati a figurare negli archivi.

2. Le disposizioni della presente direttiva non si applicano ai trattamenti di dati personali;
- effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario, come quelle previste dai titoli V e VI del trattato sull'Unione europea e comunque ai trattamenti aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato, laddove tali trattamenti siano connessi a questioni di sicurezza dello Stato) e le attività dello Stato in materia di diritto penale;
- effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico.

Entrambe le disposizioni presentano criteri rigorosi per l'applicazione a soggetti al di fuori dell'Unione Europea nel contesto del trattamento dei dati personali. La versione precedente del "*Codice della privacy*" italiano (D. Lgs. 196/2003), in particolare, utilizzava come criterio principale la presenza di strumenti di trattamento dei dati all'interno dello Stato membro, indipendentemente dalla natura dei dati stessi; infatti, prima le leggi europee sulla protezione dei dati si applicavano se un'azienda aveva strumenti per gestire dati in Europa, indipendentemente da quali dati fossero. Ora, le nuove regole dicono che le leggi si applicano solo se l'azienda ha strumenti dedicati al tipo specifico di dati che sta trattando.

Il Regolamento invece, contempla una serie di ipotesi, ai fini dell'applicazione dello stesso, ben più ampia ma comunque in grado di creare numerosi problemi interpretativi per l'interprete del diritto.[86] Le ipotesi delineate dall'articolo 5, possono essere così sintetizzate:

- Il trattamento dei dati avviene da parte di organizzazioni stabilite all'interno dell'Unione Europea, indipendentemente dal luogo effettivo in cui vengano trattati i dati personali;
- Il trattamento dei dati avviene nei confronti di interessati residenti nell'Unione Europea quando le attività di trattamento riguardano:
  – l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall' obbligatorietà di un pagamento dell'interessato;
  – il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.
- Il trattamento viene effettuato all'interno di uno Stato non Membro ma soggetto al diritto di un Paese Membro in virtù di norme di diritto internazionale.

[86] Messina A.; (2017) "*Privacy e regolamento europeo*". Milano, Edizione Ipsoa, 2019

L'applicazione del Regolamento dipende dunque dalla presenza di uno dei due seguenti criteri: il *criterio dello stabilimento* ed il *criterio dell'individuazione*.

Il *criterio dello stabilimento* stabilisce che se un'azienda è stabilita in un Paese dell'Unione Europea e sta gestendo dati in quel Paese, allora deve seguire le leggi di protezione dei dati di dell'Unione Europea. "*Stabilimento*" si riferisce a un'organizzazione stabile che sta facendo affari in modo continuativo in quel Paese. Questo criterio si riferisce al titolare o al responsabile del trattamento (l'azienda o l'organizzazione che gestisce i dati) che è situato in un Paese dell'Unione Europea. In questo caso, il Regolamento sulla protezione dei dati si applica automaticamente, indipendentemente da dove effettivamente avvenga il trattamento dei dati.[87]

La giurisprudenza della Corte di Giustizia dell'Unione Europea ha analizzato il criterio dello "*stabilimento*", all'interno di due diverse pronunce, andando a definire il perimetro di applicazione dello stesso.

Nella *Sentenza Google Spain SL (C-131/12)*,[88] la Corte di Giustizia dell'Unione Europea ha ampliato la portata territoriale della direttiva 95/46/CE per garantire ai dati dei cittadini europei, anche se trattati al di fuori dell'Unione Europea, le stesse protezioni previste per i dati trattati all'interno dell'Unione. In altre parole, la Corte ha stabilito che non è tanto importante dove esattamente avviene il trattamento dei dati fisicamente, ma piuttosto dove l'azienda che gestisce il trattamento ha la sua base operativa. Nel caso specifico, la Corte ha osservato che Google Spain, una filiale di Google Inc. con sede negli Stati Uniti, è considerata uno "stabilimento" ai sensi della Direttiva perché opera in Spagna. Pertanto, quando i dati vengono trattati per le

[87] Vanegas J. G.; "*La violazione dei requisiti di sicurezza informatica di cui all'art 32 del GDPR*", pubblicato su "Il diritto dell'informazione e dell'informatica" Fascicolo 2-2020

[88] Il testo integrale, in lingua italiana, della Sentenza della Corte di Giustizia dell'Unione Europea, Causa C-131/12, Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), 14 maggio 2014 [Online] Consultabile su http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=it&mode=lst&dir=&occ=first&part=1&cid=1009308

attività di un motore di ricerca gestito da un'azienda con una filiale in uno Stato membro dell'Unione Europea, il trattamento viene considerato come svolto "nel contesto delle attività" di quella filiale.[89] Questo vale anche se il servizio di ricerca stesso è gestito da un'azienda situata al di fuori dell'Unione Europea.

Nella *Sentenza Weltimmo c. NAIH (C-230/14)*,[90] la Corte di Giustizia dell'Unione Europea ha confermato un principio simile a quello stabilito nella Sentenza Google Spain. Sebbene i casi fossero diversi (Google Spain riguardava l'applicabilità delle leggi sulla protezione dei dati ai trattamenti effettuati al di fuori dell'Unione Europea, mentre Weltimmo affrontava la questione di quale legislazione nazionale si dovesse applicare quando un trattamento di dati aveva luogo in due Stati Membri diversi), entrambe le sentenze si sono concentrate sull'interpretazione del concetto di "stabilimento". La controversia nella Sentenza Weltimmo c. NAIH (C-230/14) riguardava il fatto che la Weltimmo, con sede in Slovacchia, aveva raccolto dati personali di cittadini ungheresi attraverso il suo portale web per annunci immobiliari, senza rispettare adeguatamente le leggi ungheresi sulla protezione dei dati. Nonostante appunto la sede principale fosse in Slovacchia, l'azienda aveva attività che coinvolgevano cittadini ungheresi, e questo ha portato all'azione legale da parte dell'autorità di protezione dei dati ungherese (NAIH). La questione principale era se l'azienda slovacca dovesse rispettare le leggi ungheresi sulla protezione dei dati quando raccoglieva dati personali di cittadini ungheresi tramite il suo servizio online.

In entrambi i casi, la Corte ha sottolineato che la direttiva sulla protezione dei dati non richiede che il trattamento dei dati personali sia effettuato dallo stesso stabilimento coinvolto, ma

[89] Finocchiaro G., "*La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*" pubblicato su "Il diritto dell'informazione e dell'informatica" Anno XXX Fasc. 4-5 -2015
[90] Il testo integrale, in lingua italiana, della Sentenza della Corte di Giustizia dell'Unione Europea, Causa C-230/14, Weltimmo 1 Consultabile su
http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=IT

piuttosto che avvenga nel contesto delle attività di quell'organizzazione. Questo significa che la legge sulla protezione dei dati di uno Stato membro diverso da quello in cui è registrato il responsabile del trattamento può essere applicata, a condizione che l'organizzazione abbia un'attività effettiva e reale, anche minima, nel territorio di quel secondo Stato membro in cui si svolge il trattamento dei dati.[91]

Il *criterio dell'individuazione* invece, si basa sul luogo in cui si trovano le persone interessate dal trattamento dei dati. Il Regolamento si applica se il titolare del trattamento è situato al di fuori dell'Unione europea, ma le sue attività coinvolgono sia l'offerta di beni o servizi a persone che si trovano nell'Unione, sia il monitoraggio del comportamento di queste persone all'interno dell'Unione. In altre parole, il Regolamento si applica se un residente di un Paese europeo, indipendentemente dalla sua nazionalità, è soggetto a un trattamento dei dati.

Per determinare se il Regolamento si applica, è necessario valutare ciascun caso individualmente, tenendo conto dell'intenzione del titolare del trattamento di offrire beni o servizi alle persone che si trovano nell'Unione o di monitorare il loro comportamento.[92]

In sostanza, l'applicazione extraterritoriale del GDPR sembra conferire alla legge un'ampia portata geografica, ma in realtà rappresenta un potenziamento della protezione dei soggetti interessati attraverso l'espansione delle situazioni di trattamento coperte dal regolamento. A tal proposito è importante notare infatti, che gli individui interessati devono comunque trovarsi nell'Unione Europea per beneficiare delle disposizioni di rafforzamento dei loro diritti ai sensi del regolamento. Quindi, il GDPR europeo sembra sovrapporsi solo in apparenza alle leggi nazionali di paesi al di fuori dell'Europa, poiché la sua giurisdizione rimane limitata all'Unione

[91] Finocchiaro G., "*La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*" pubblicato su "Il diritto dell'informazione e dell'informatica" Anno XXX Fasc. 4-5 -2015
[92] Marini, P.; "*GDPR: il nuovo regolamento europeo sulla privacy*". Milano: Edizione Ipsoa. 2017, p. 52

Europea e mira principalmente a proteggere chiunque sia soggetto a un trattamento all'interno del territorio europeo.[93]

4. I PRINCIPI DEL GDPR APPLICABILI AL TRATTAMENTO DEI DATI

A) I principi di liceità, correttezza e trasparenza

Il Capo II del Regolamento 2016/679, che si estende dall'articolo 5 all'articolo 11, è focalizzato sui "*Principi*". L'articolo 5 di questo regolamento, intitolato "*Principi applicabili al trattamento dei dati personali*", raccoglie un elenco completo dei principi che regolamentano questa tematica. Data la sua notevole rilevanza, è opportuno riportarlo integralmente:

Articolo 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");

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali ("limitazione della finalità");

[93] Cfr. D'Anna A.; "*L'ambito di applicazione territoriale del regolamento generale per la protezione dei dati personali*", Horisma, 2019, p. 61-83 a cura di Bonavita S.; "*Società delle tecnologie esponenziali e general data protection regulation: la circolazione internazionale dei dati personali"*

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza");

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato ("limitazione della conservazione");

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ("integrità e riservatezza").

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

Questo articolo rappresenta un punto fondamentale per l'intero sistema posto in piedi dal GDPR, dato che sulla base dei su principi vengono poi radicati gli ulteriori diritti e obblighi spettanti ai soggetti che operano in tale settore.

L'art. 5 stabilisce fin da subito che i dati devono essere trattati in modo *lecito, corretto* e *trasparente* nei confronti dell'interessato.

Il trattamento dei dati personali è considerato *lecito* quando rispetta la normativa vigente, si basa sul consenso dell'individuo interessato e risponde alla necessità del trattamento. I presupposti di liceità sono definiti all'articolo 6 del Regolamento,[94] il quale ad esempio stabilisce che il trattamento è considerato lecito quando è necessario per eseguire un contratto in cui l'individuo interessato è coinvolto, per proteggere gli interessi vitali dell'interessato o di un'altra persona fisica, quando è richiesto per adempiere a un obbligo legale o per perseguire un interesse legittimo del responsabile del trattamento o di terze parti. In sostanza è importante che il titolare del trattamento sia in grado di dimostrare che ha una base giuridica valida per il trattamento e che rispetta tutte le normative pertinenti per garantire che il trattamento sia effettuato in modo legittimo e responsabile. Con il principio di *correttezza* si intende che i dati personali devono essere trattati in modo accurato e aggiornato quando necessario. Alcuni punti chiave relativi a questo principio includono:

- **Precisione dei dati:** I dati personali devono essere accurati e veritieri. È responsabilità del titolare del trattamento assicurarsi che i dati siano corretti e aggiornati, e deve prendere misure per correggere eventuali informazioni errate.
- **Limitazione della conservazione:** I dati personali devono essere conservati solo per il tempo necessario alle finalità per le quali sono stati raccolti. Ciò significa che i dati non dovrebbero essere conservati più a lungo di quanto sia necessario.
- **Sicurezza dei dati:** Il trattamento dei dati deve includere misure di sicurezza adeguate per proteggere i dati personali da accessi non autorizzati o divulgazioni indebite. Questo contribuisce a garantire che i dati rimangano corretti e riservati.

[94] Art. 6 GDPR

- **Aggiornamenti:** Se i dati personali cambiano o diventano obsoleti, devono essere aggiornati di conseguenza. Ciò garantisce che i dati siano sempre corretti e pertinenti alle finalità del trattamento.[95]

Il *principio della trasparenza* richiede che le informazioni e le comunicazioni relative al trattamento dei dati personali siano facilmente accessibili e comprensibili, utilizzando un linguaggio semplice e chiaro. Questo principio si concentra sull'informazione degli interessati riguardo all'identità del titolare del trattamento, alle finalità del trattamento e ad altre informazioni necessarie per garantire un trattamento corretto e trasparente dei loro dati personali. È importante sensibilizzare le persone sui rischi, sulle norme, sulle garanzie e sui diritti legati al trattamento dei dati personali, nonché sulle modalità per esercitare tali diritti.[96]

B) Il principio della finalità nel trattamento dei dati

I principi sopra esposti cercano in qualche modo di porre al riparo i soggetti i cui dati vengono trattati attribuendo loro delle garanzie che gli permettano di tutelarsi in modo migliore in un mondo sempre più guidato dai dati.

I profili di maggiore rischio emergono quale conseguenza dell'acquisizione e utilizzo di dati personali attraverso l'utilizzo di algoritmi complessi i cui processi decisionali sono spesso opachi. Infatti davanti alla presenza di c.d. Big Data le tecniche di analisi sono complesse e come tali non semplici da spiegare all'interessato in modo tale da garantire la consapevolezza delle conseguenze relative al trattamento dei propri dati personali attraverso tali sistemi. In sostanza non è sempre possibile prevedere fin dall'inizio tutti gli usi che possono essere fatti di tali dati.[97]

[95] D'Avanzo W.; "*Lotta alla pandemia e tutela della privacy*" Tigor: rivista di scienze della comunicazione e di argomentazione giuridica - A. XIV (2022) n.2
[96] Cfr. Considerando 39 GDPR
[97] Turilli M.; "*The ethics of information transparency, in Ethics and Information Technology*", 2009, p. 11ss.

Accade dunque che spesso non è possibile fornire in anticipo una spiegazione dettagliata su come verranno trattati i dati in modo che la persona interessata possa dare il proprio consenso in modo informato e corretto. Questo crea una situazione in cui c'è una mancanza di informazioni paritaria tra la persona interessata e il responsabile del trattamento dei dati.[98]

La difficoltà di prevedere l'utilizzo e i risultati dei dati personali comporta problematiche non solo in ambito di trasparenza e consenso informato, ma anche per quanto concerne la limitazione delle *finalità di trattamento.*

Come evidenziato dal gruppo di lavoro "Articolo 29",[99] è essenziale garantire che anche nell'ambito dei Big Data venga rispettato il principio di finalità, assicurando che le finalità del trattamento dei dati rientrino nelle aspettative delle persone interessate. Questo principio ha due obiettivi principali. Innanzitutto, assicura il rispetto dei diritti degli individui, mantenendo un equilibrio con gli interessi delle aziende. Inoltre, serve a prevenire lo sviluppo di monopoli e situazioni di dominanza nel campo dell'analisi dei dati. Ecco che dunque per garantire il principio di finalità, è importante informare le persone interessate durante la raccolta e l'analisi dei dati se le finalità del trattamento differiscono da quelle iniziali.[100]

Tuttavia, esistono delle situazioni eccezionali in cui il principio di limitazione delle finalità può essere superato, consentendo un ulteriore trattamento dei dati personali. Questo trattamento aggiuntivo è ammesso solo se è finalizzato all'archiviazione nell'interesse pubblico,[101] a scopi di ricerca scientifica o storica,[102] o a scopi statistici.[103] È importante notare che questa

[98] McDonald A.M.; " *The Cost of Reading Privacy Policies*" in I/S: A Journal of Law and Policy for the Information Society, p. 4ss

[99] Gruppo di lavoro "Articolo 29", *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU*, Settembre 2012.

[100] De Gregorio.; "*Privacy, tutela dei dati personali e Big Data",* Milano, 2022, p. 27

[101] Cfr. Considerando 158 GDPR

[102] Cfr. Considerando 159 GDPR

[103] Cfr. Considerando 162 GDPR

eccezione deve essere applicata solo se sono in atto "*garanzie adeguate*" per proteggere i diritti e le libertà delle persone interessate, come previsto dall'articolo 89 del regolamento.[104]

C) Ulteriori principi: minimizzazione dei dati, conservazione e accuratezza

Partendo dai principi precedentemente esaminati, è evidente come la raccolta e l'analisi di enormi volumi di dati abbiano un impatto profondo sul principio della *minimizzazione dei dati*. Questo principio, noto anche come il concetto di proporzionalità, necessità e non eccedenza rispetto alla quantità di dati da trattare, rappresenta uno dei pilastri fondamentali della protezione dei dati personali nell'era digitale.

Nel contesto tradizionale dell'analisi dei dati, la prassi era quella di considerare solo i dati giudicati immediatamente rilevanti per uno specifico scopo. Tuttavia, con l'avvento dei Big Data, si è assistito a un profondo cambiamento di prospettiva. Qui, l'approccio è diverso, poiché si riconosce che persino i dati inizialmente considerati non essenziali possono rivelare informazioni preziose quando sono inclusi in un quadro più ampio.

Questa caratteristica peculiare dei Big Data è resa possibile dalla crescente capacità di memorizzare e analizzare quantità smisurate di dati. Le tecnologie avanzate, come l'archiviazione cloud e gli algoritmi di analisi dei dati, consentono alle organizzazioni di acquisire, conservare e processare dati su una scala mai vista prima. Inoltre, l'accesso a un vasto patrimonio di dati è diventato sempre più accessibile. Tuttavia, ciò solleva alcune importanti considerazioni etiche e legali. Mentre la raccolta e l'analisi di dati massicci possono offrire benefici significativi in termini di scoperta di modelli, innovazione e miglioramento dei servizi, è essenziale garantire che i diritti e le privacy delle persone siano adeguatamente protetti. Pertanto, il principio della minimizzazione dei dati rimane fondamentale. Significa che,

[104] Cfr. Art 89 GDPR

nonostante la disponibilità di enormi quantità di dati, le organizzazioni devono raccogliere solo i dati strettamente necessari per scopi specifici e dichiarati in anticipo.[105]

Un ulteriore aspetto cruciale e interconnesso riguarda la gestione e la *conservazione* dei dati personali. Il GDPR stabilisce chiaramente che i dati personali devono essere conservati in una forma che permetta l'identificazione degli individui solo per il tempo strettamente necessario per raggiungere le finalità per le quali sono stati raccolti.[106] Questo principio, noto come limitazione della conservazione, sottolinea la necessità di non trattenere i dati più a lungo di quanto sia giustificato dallo scopo iniziale del trattamento.

Sotto lo stesso profilo, il fenomeno dei Big Data coinvolge anche il *principio di accuratezza*. Se si prendono ad esempio le tecniche di data mining, è possibile notare come le modalità con cui i dati vengono raccolti non riescono a garantire un esatto rispetto di tale principio.

Il data mining utilizza varie fonti come i social media e altre fonti di terze parti dalle quali sarà difficile accertare l'accuratezza dei dati. L'incremento delle fonti di provenienza dei dati è direttamente proporzionale all'aumento del rischio di trattare dati inaccurati. Tale problema non si presenta soltanto ex ante in fase di raccolta e analisi ma anche ex post per via degli effetti distorti che i dati inaccurati possono avere sugli output.[107]

4.1 I diritti dell'interessato

Il Capo III riguarda i "*Diritti dell'interessato*" alcuni sono introdotti ex novo, altri invece vengono meglio definiti rispetto al passato.

[105] Bygrave L.A.; "*Data Protection Law: Approaching Its Rationale, Logic and Limits",* The Hague, 2002, p. 85ss
[106] Cfr. Art. 4 GDPR
[107] De Gregorio.; *Privacy, tutela dei dati personali e Big Data,* Milano, 2022, p. 29

A) Il diritto all'informazione

La prima norma del Capo riguarda l'Articolo 12, il quale enfatizza e dettaglia il "*Diritto all'informazione*". Questo diritto è strettamente legato all'obbligo di trasparenza già analizzato nelle pagine precedenti. I punti salienti di questa disposizione sono:

- Il responsabile del trattamento è tenuto a fornire all'individuo interessato informazioni dettagliate sulle operazioni di trattamento in modo che siano "*concise, trasparenti, facilmente comprensibili, e facilmente accessibili, utilizzando un linguaggio semplice e chiaro*".[108] Questo vale in particolare se la persona interessata è un minore. L'obiettivo principale è garantire che l'individuo comprenda appieno cosa accadrà ai suoi dati e possa facilmente esercitare i propri diritti.
- Le informazioni riguardanti il trattamento dei dati devono essere comunicate per iscritto o attraverso mezzi elettronici. L'informativa verbale è consentita solo in due circostanze: se l'individuo interessato ne fa esplicita richiesta e se la sua identità non può essere verificata mediante altri mezzi.[109]
- La normativa prevede che se il titolare del trattamento non adempie alla richiesta dell'interessato, deve notificarlo tempestivamente (entro un mese) riguardo alle ragioni per cui non è stato dato seguito alla richiesta. Inoltre, l'interessato deve essere informato sulla possibilità di presentare un reclamo all'autorità nazionale di controllo e di avviare un'azione legale.[110]
- La normativa stabilisce che se le richieste dell'interessato sono chiaramente infondate o eccessive, soprattutto se sono di natura ripetitiva, il titolare del trattamento può

[108] Cfr. Art 12 paragrafo 1 GDPR
[109] Cfr. Art 12 paragrafo 1 GDPR
[110] Cfr. Art 12 paragrafo 4 GDPR

rifiutarsi di rispondere alla richiesta. In questo caso, è il titolare del trattamento che deve dimostrare la validità della sua decisione.[111]

B) Il diritto d'accesso

L'articolo 15, noto come "*Diritto di accesso dell'interessato*",[112] stabilisce che una persona ha il diritto di richiedere al titolare del trattamento la conferma che vengano trattati o meno dati personali che la riguardano. In caso di trattamento, ha il diritto di accedere a tali dati personali e ottenere ulteriori informazioni specificate nel paragrafo 1.[113]

Il diritto in questione era disciplinato anche all'articolo 12 lettera a) della Direttiva 95/46/CE;[114] rappresenta però quel tipo di disposizione citato poc'anzi del quale il GDPR dà una disciplina più dettagliata.

C) Il diritto all'oblio

La direttiva 95/46/CE non includeva disposizioni specifiche relative al "*diritto all'oblio*", ma questa tematica è stata affrontata nel Regolamento al suo articolo 17, intitolato "*diritto alla cancellazione dei dati personali (diritto all'oblio)*".[115] Tuttavia, è importante notare che l'articolo menziona solo il "diritto di cancellazione", senza fare riferimenti espliciti al "diritto all'oblio". È fondamentale comprendere che il "diritto all'oblio" non coincide né può essere ridotto al "diritto di cancellazione", poiché quest'ultimo rappresenta solo una delle modalità operative del primo.[116] Se considerassimo il "diritto all'oblio" come una semplice estensione

[111] Cfr. Art 12 paragrafo 5 GDPR
[112] Cfr. Art. 15 GDPR
[113] Tra le informazioni dell'Articolo 15 paragrafo 1 troviamo, a titolo esemplificativo: le finalità del trattamento, le categorie di dati personali in questione, i destinatari a cui i dati personali sono stati o saranno comunicati, il periodo di conservazione dei dati personali previsto
[114] Cfr. Art 12 Direttiva 95/46/CE
[115] Alù A.; "*Esiste il diritto all'oblio su internet? La complessa evoluzione di tale figura tra giurisprudenza e legge"*, in Diritto di famiglia e delle persone, n.1, 2020, 2, p. 313-328
[116] Di Ciommo F.; *Il diritto all'oblio (oblito) nel Regolamento (UE) 2016/679 sul trattamento dei dati personali,* in Foro Italiano, fasc. 6, settembre 2017

del "*diritto di cancellazione*", ne perderemmo il significato profondo. Quindi, si crea una confusione tra concetti differenti, e questa confusione potrebbe essere attribuita alla natura stessa del World Wide Web, dove le informazioni indicizzate dai motori di ricerca rimangono accessibili in modo permanente a un pubblico indeterminato di utenti.[117]

Fatta questa precisazione l'art 17 al primo comma indica le ipotesi che permettono all'interessato di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano e l'obbligo del titolare del trattamento di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:; se l'interessato revoca il consenso e non sussiste un altro fondamento giuridico per il trattamento; quando vi è opposizione da parte dell'interessato e non sussiste alcun motivo legittimo prevalente per procedere al trattamento; se i dati sono stati trattati illecitamente; quando sussiste un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; infine nel caso in cui i dati sono stati raccolti relativamente all'offerta di servizi della società dell'informazione a un minore.[118]

Alla luce del testo normativo, è importante sottolineare che l'ambito di applicazione della cancellazione come strumento per garantire il diritto all'oblio sarà, in parte, definito dall'interprete del diritto. Quest'ultimo ha il compito di elaborare il concetto di "*sopravvenuta mancanza di necessità rispetto alle finalità originarie*" e di stabilire quanto siano ampi i "*legittimi motivi prevalenti*".

La norma richiede, infatti, un processo di bilanciamento degli interessi coinvolti in ogni situazione specifica. Questo processo deve tener conto delle circostanze particolari del caso e deve essere condotto in modo concreto. In altre parole, il Regolamento fornisce linee guida

[117] Palmieri A.; "*Dal diritto all'oblio all'occultamente in rete*", in Foro it., 2014, p.1- 16
[118] Art 17 primo comma GDPR

generali, ma la sua applicazione pratica richiede una valutazione dettagliata delle circostanze, tenendo conto delle diverse variabili in gioco.[119]

Il comma due per una migliore comprensione lo si può collegare al considerando 66 del Regolamento; viene così stabilito che per rafforzare il diritto all'oblio nell'ambiente online, è opportuno che il diritto di cancellazione sia esteso in modo tale da obbligare il titolare del trattamento che ha pubblicato i dati personali a informare i titolari del trattamento che trattano tali dati personali di cancellare qualsiasi link verso tali dati personali o copia o riproduzione di detti dati personali. Nel fare ciò, è opportuno che il titolare del trattamento adotti misure ragionevoli tenendo conto della tecnologia disponibile e dei mezzi a disposizione del titolare del trattamento, comprese misure tecniche, per informare della richiesta dell'interessato i titolari del trattamento che trattano i dati personali.
In conformità con il terzo comma dell'articolo 17, la cancellazione dei dati personali non si applica in una serie di situazioni. In particolare, questa eccezione viene applicata in casi in cui il trattamento dei dati è "*necessario per l'esercizio della libertà di espressione e di informazione*". Tuttavia, è importante notare che questa eccezione non è assoluta e generale.

La sua applicabilità dipende da vari fattori, come l'attualità della notizia e la presenza di basi e criteri validi per l'esercizio corretto del diritto di informazione. Se questi requisiti non sono soddisfatti o non sono più validi, l'eccezione prevista nel terzo comma non si applica, e l'individuo può richiedere la tutela del diritto all'oblio. In altre parole, l'eccezione alla cancellazione dei dati personali è limitata e soggetta a valutazioni specifiche delle circostanze.[120]

[119] Bellomia V.; "*Diritto all'oblio e la società dell'informazione*", p. 244
[120] Bellomia V.; "*Diritto all'oblio e la società dell'informazione*", p. 245ss

L'applicazione del diritto all'oblio può essere limitata anche in altre circostanze. Ad esempio, la conservazione dei dati personali può essere necessaria per adempiere agli obblighi previsti dal diritto comunitario o nazionale, per ragioni di interesse pubblico nel campo della sanità e per scopi legati all'accertamento, all'esercizio o alla difesa di un diritto in sede giudiziaria. Inoltre, il considerando 73 del GDPR prevede la possibilità di ulteriori limitazioni che possono essere stabilite dagli Stati membri. Queste limitazioni devono comunque rispettare il principio di necessità e proporzionalità. L'obiettivo di tali limitazioni è proteggere la sicurezza pubblica e altri interessi generali dell'Unione europea o di uno Stato membro.

Va sottolineato che la protezione del diritto all'oblio secondo il GDPR non si limita all'articolo 17. Al contrario, altri articoli come il 16 ("*diritto di rettifica*") e il 18 ("*diritto di limitazione al trattamento*") contribuiscono a garantire e arricchire la tutela di questo diritto.[121]

L'articolo 16 del Regolamento europeo stabilisce che «*l'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa*».

Questo diritto permette all'individuo di mantenere un controllo diretto sui propri dati, consentendogli di richiedere correzioni, modifiche, integrazioni e aggiornamenti. In questo modo, si assicura che la personalità attuale dell'individuo sia rispettata, considerandola nel contesto attuale e non ancorata a eventi passati. Il considerando 65 del Regolamento affronta

[121] Napolitano C., "*Il diritto all'oblio: la centralita' dell'identita' personale*", in Danno e Resp., n. 6, 2020, p. 732

contemporaneamente il diritto alla rettifica e il diritto alla cancellazione poiché entrambi mirano a proteggere la reputazione online e la personalità digitale delle persone.[122]

Ai sensi dell'articolo 18 del GDPR, l'interessato può chiedere la sospensione temporanea della gestione dei suoi dati personali, il blocco del trattamento, nei seguenti casi: violazione del principio di liceità, mancato rispetto del principio di esattezza dei dati, presentazione di richiesta di rettifica in attesa di effettuazione, opposizione al trattamento in attesa di decisione del titolare. Non appena il titolare del trattamento riceve la richiesta dell'interessato, deve marcare i dati oggetto della suddetta richiesta, apporre cioè il contrassegno, al fine di distinguerli dagli altri dati, non oggetto di limitazione. In caso di esercizio di tale diritto ogni trattamento, tranne la conservazione, è vietato a meno che sia stato prestato il consenso dell'interessato al trattamento per scopi diversi, o esso sia necessario per l'esercizio o la difesa di un diritto in sede giudiziaria, per la tutela dei diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante.[123]

D) Il diritto di opposizione

Un ulteriore diritto che può anche esso essere collegato al diritto all'oblio è il diritto di opposizione, disciplinato all'articolo 21 del Regolamento: "*l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano*". Nel caso venga esercitato tale diritto, il titolare deve astenersi dal trattare i dati dell'interessato, a meno che questo risulti necessario per l'esistenza di motivi legittimi cogenti che prevalgono sui diritti e sulle libertà dell'interessato, nonché per l'esercizio o la difesa di un diritto in sede giudiziaria.

[122] Cfr. Considerando 65 GDPR
[123] Cfr. art 18 GDPR

La sua attuazione solleva una serie di questioni pratiche e concettuali di notevole rilevanza. Una delle sfide principali consiste nella definizione di cosa costituisca una "*situazione particolare*" e quali siano i "*motivi connessi*" che giustificano l'esercizio di questo diritto. La flessibilità di questa formulazione mira a garantire che il diritto all'opposizione possa essere esercitato in una vasta gamma di circostanze, ma allo stesso tempo richiede una valutazione caso per caso.[124]

Un'altra questione cruciale riguarda le limitazioni al diritto all'opposizione. Il GDPR stabilisce che tale diritto può essere limitato se il titolare del trattamento dimostra che ci sono "*motivi legittimi prevalenti*" per continuare il trattamento che superano gli interessi, i diritti e le libertà dell'individuo opponente. Questa formulazione apre la strada a diverse interpretazioni e richiede un delicato esercizio di bilanciamento tra i diritti dell'individuo e gli interessi dell'organizzazione.

Da un punto di vista pratico, le organizzazioni devono essere preparate a gestire le richieste di opposizione in modo efficace e tempestivo. Questo implica la necessità di avere procedure chiare per ricevere, valutare e rispondere a tali richieste. Inoltre, le aziende devono essere in grado di dimostrare che rispettano il diritto all'opposizione e che stanno effettivamente considerando i motivi connessi alla situazione particolare dell'individuo.[125]

E) Il diritto alla portabilità dei dati

Il diritto alla portabilità costituisce una delle innovazioni più rilevanti apportate dal Regolamento generale sulla protezione dei dati. La sua essenza è chiara: garantisce a ciascun individuo che usufruisce di servizi online il diritto di "trasportare" i propri dati da un servizio

[124] Napolitano C., "*Il diritto all'oblio: la centralita' dell'identita' personale*", in Danno e Resp., n. 6, 2020, p. 732ss
[125] Bellomia V.; "*Diritto all'oblio e la società dell'informazione*", p. 250ss

all'altro. Questo consente di riutilizzare autonomamente le proprie informazioni senza perdere il prezioso patrimonio di dati precedentemente creato. Un esempio tipico riguarda l'uso di piattaforme online come i social network, che raccolgono una vasta quantità di dati personali, informazioni e contenuti multimediali dagli utenti. Il nuovo diritto alla portabilità consente all'utente di ottenere una copia dei propri dati e archiviarli nel proprio computer, oppure trasmetterli ad un'altra piattaforma per essere riutilizzati. La norma introdotta dalla legislazione europea è estremamente ampia nel suo campo di applicazione, coinvolgendo tutti i soggetti che effettuano il trattamento elettronico dei dati personali. Indipendentemente dal tipo di servizio fornito e dalle dimensioni dell'impresa, questa disposizione si applica a un ampio spettro di attori, che vanno dalle grandi piattaforme di e-commerce ai servizi di archiviazione cloud, fino alle applicazioni per smartphone sviluppate da piccole start-up. In altre parole, qualsiasi impresa che si occupi del trattamento di dati personali deve garantire ai propri utenti il diritto alla portabilità dei loro dati.

La ratio di questa norma è rafforzare i diritti individuali all'interno di un contesto digitale sempre più centrato sull'utilizzo commerciale dei dati personali. In questo contesto, essa sottolinea il principio che i dati personali appartengono alle persone anche quando sono in possesso di terzi, e che ogni individuo deve avere il controllo completo sulla destinazione e sull'utilizzo dei propri dati personali.[126]

Il GDPR disciplina tale diritto all'articolo 20;[127] L'applicazione del diritto è determinata da tre elementi interconnessi. Inizialmente, essa dipende dal tipo di dati sui quali viene esercitato, le modalità con le quali è disciplinata la sua attuazione e i limiti imposti al suo esercizio.

[126] Borghi M.; "*Portabilità dei dati e regolazione dei mercati digitali*" in Mercato concorrenza regole / a. XX, n. 2, agosto 2018, p. 228ss
[127] Cfr. Art. 20 GDPR

Per quanto riguarda *i dati oggetto di portabilità* Il diritto alla portabilità si esercita su «d*ati personali che [...] riguardano*» un interessato, e che siano stati «*forniti*» dallo stesso interessato «*a un titolare del trattamento*».[128] La prima condizione esclude i dati che non riguardino una persona fisica, come ad esempio quelli che si riferiscono a un'attività commerciale, un'impresa o un'organizzazione. La seconda esclude i dati che non riguardano la persona che chiede di esercitare il diritto alla portabilità. Rientrano in questa fattispecie non solo i dati riguardanti altre persone, ma anche quelli resi completamente anonimi, cioè non più idonei a identificare una persona fisica.[129] La seconda condizione richiede poi un'ulteriore qualificazione; si riferisce infatti solamente a quei dati forniti dall'interessato che siano trattati, con mezzi automatizzati, o sulla base del consenso dell'interessato o nell'esecuzione di un contratto sottoscritto dall'interessato.

L'articolo 20 impone poi condizioni specifiche quanto al *modo* in cui l'interessato deve ricevere i dati dal titolare del trattamento; tre sono le componenti da considerare: l'interessato ha innanzitutto il diritto di ricevere i dati in un formato interoperabile, che ne consenta cioè il riutilizzo in altri sistemi; ha quindi il diritto di trasmetterli a un altro titolare «*senza impedimenti*»; e infine ha il diritto di ottenere la trasmissione diretta da un titolare all'altro «*se tecnicamente fattibile*». Il concetto di portabilità dei dati si salda qui con quello di interoperabilità, ossia la possibilità di trasferire dati e informazioni in generale da un sistema, un'applicazione o un dispositivo a un altro, e di utilizzarli su ciascuno di essi.[130]

Da ultimo va sottolineato come l'art. 20 GDPR stabilisce che l'esercizio di tale diritto è soggetto alla condizione che «*non deve ledere i diritti e le libertà altrui*». Come chiarito nel

[128] Art. 20 GDPR
[129] Cfr. Gruppo di Lavoro articolo 29, Parere 05/2014 sulle tecniche di anonimizzazione, adottato il 10 aprile 2014
[130] Ferretti F.; "*Data protection and the legitimate interest of data controllers: much Ado about nothing or the winter of rights?*", in «Common Market Law Review», 2014 p. 512

Considerando 68, la limitazione riguarda innanzitutto gli altri individui i cui dati siano eventualmente condivisi con colui che esercita il diritto alla portabilità, ad esempio perché gli stessi dati riguardano più persone. Inoltre, il trasferimento dei dati non deve pregiudicare altri diritti previsti dal GDPR, come ad esempio il diritto di accesso, rettifica e cancellazione. In questo senso, il titolare del trattamento può opporsi a una richiesta di trasferimento diretto a un altro titolare non soltanto quando non sia tecnicamente fattibile, ma anche quando tale trasferimento possa compromettere diritti e libertà di altri interessati.[131]

4.2 Gli obblighi e le responsabilità del titolare e del responsabile del trattamento

A) Il titolare e il responsabile del trattamento: le definizioni del GDPR

Il Capo IV, intitolato "*Titolare del trattamento e responsabile del trattamento*," si apre con l'articolo 24, che riguarda la "*Responsabilità del titolare del trattamento.*" Il titolare del trattamento, come definito nell'articolo 4 del Regolamento, è il soggetto che determina le modalità, le finalità e le scelte operative relative al trattamento dei dati ed è quindi la figura principale coinvolta nel processo di trattamento dei dati.[132]

L'articolo 24 stabilisce chiaramente che il titolare del trattamento deve adottare misure tecniche e organizzative adeguate per garantire e dimostrare che le operazioni di trattamento siano conformi alle disposizioni del regolamento. Queste misure dovrebbero essere basate su una valutazione della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché sulla valutazione dei rischi per i diritti e le libertà delle persone fisiche.[133]

[131] Cfr. Considerando 68 GDPR
[132] Cfr. Art. 4 GDPR
[133] Cfr. Art. 24 GDPR

Al paragrafo 3 l'articolo 24 sottolinea che il titolare del trattamento può utilizzare l'adesione a codici di condotta (articolo 40 del Regolamento) e/o ai meccanismi di certificazione (articolo 42 del Regolamento) come prova del rispetto degli obblighi e della conformità alle disposizioni del regolamento.

L'articolo 24 nel suco complesso delinea chiaramente una forte responsabilità del titolare del trattamento e mette l'accento sulla prevenzione dei danni attraverso misure tecniche e organizzative adeguate, piuttosto che sulla semplice riparazione degli illeciti. La disposizione si basa sull'analisi del rischio e dell'eventuale danno causato, obbligando il titolare del trattamento a dimostrare che il trattamento sia conforme al regolamento mediante l'attuazione di adeguate misure.[134]

Il Responsabile del trattamento, come definito nell'articolo 4 n. 8 del Regolamento, è una "*persona fisica o giuridica(...)che tratta dati personali per conto del titolare del trattamento*."[135] La sua funzione è strettamente legata all'operato del titolare del trattamento e viene attivata solo quando il trattamento dei dati personali deve essere effettuato per conto del titolare.

L'articolo 28 del Regolamento stabilisce che il titolare può avvalersi dei servizi del responsabile solo se quest'ultimo è in grado di fornire garanzie sufficienti per adottare misure tecniche e organizzative adeguate a soddisfare i requisiti regolamentari e proteggere i diritti degli interessati. Questa relazione tra titolare e responsabile, nonché i trattamenti condotti dal responsabile, devono essere regolati da un contratto o altro atto giuridico, stipulato in forma scritta o elettronica, che definisca chiaramente la materia disciplinata, la durata, la natura e la

[134] Riccio. M.; "*Data Protection Officer e altre figure*" in "*La Nuova Disciplina Europea della Privacy"*, a cura di Sica S., D'Antonio, Riccio M., Milano, 2016, pag. 41ss
[135] Cfr. Art. 4 paragrafo 8 GDPR

finalità del trattamento, la tipologia di dati personali e la categoria di interessati, nonché gli obblighi e i diritti del titolare del trattamento.[136]

Il ruolo principale del responsabile è di fornire supporto alle funzioni e mansioni del titolare, seguendo le disposizioni del titolare come specificate nel contratto. Questo supporto, come precisa il paragrafo 3 dell'articolo 28, include l'assistenza nella predisposizione di misure tecniche e organizzative per rispondere alle richieste di esercizio dei diritti da parte degli interessati, garantendo il rispetto degli obblighi di sicurezza previsti dall'articoli 32-36, e la cancellazione o restituzione dei dati personali al termine dei servizi, a meno che ciò sia vietato dal diritto dell'Unione o di uno Stato membro. Inoltre, il responsabile deve mettere a disposizione del titolare tutte le informazioni necessarie per confermare la conformità alle disposizioni regolamentari e consentire o contribuire a revisioni e ispezioni richieste dal titolare o autorizzate da quest'ultimo.[137]

Il Regolamento prevede anche la possibilità per il responsabile di ricorrere a un altro responsabile, previa autorizzazione scritta, specifica o generale, da parte del titolare. In questo caso, si instaura un rapporto tra il responsabile iniziale e il sub-responsabile, simile a quello tra titolare e responsabile, con un accordo che riprende i contenuti previsti dall'articolo 28. Tuttavia, se il sub-responsabile non adempie ai propri obblighi specifici in materia di protezione dei dati, la responsabilità principale ricade comunque sul responsabile iniziale nei confronti del titolare del trattamento.

[136] Cfr. Art. 28 GDPR
[137] Cfr. Art. 28 paragrafo 3

B) Gli obblighi e le responsabilità

Per quanto riguarda gli obblighi e le responsabilità del titolare e del responsabile del trattamento, possiamo ancora una volta fare riferimento al Regolamento stesso; infatti in chiusura della Sezione I troviamo altre due importante disposizioni, l'articolo 30 e il 31.

All'articolo 30 del Regolamento è stabilito che il titolare del trattamento, e quando possibile il suo rappresentante, deve adempiere all'obbligo di mantenere un registro delle attività di trattamento effettuate sotto la sua responsabilità. Questa disposizione ha chiaramente l'obiettivo principale di agevolare il controllo e la supervisione da parte delle autorità di protezione dei dati, specialmente nel caso in cui richiedano al titolare del trattamento chiarimenti o informazioni relative ai trattamenti condotti. L'obbligo di mantenere un registro delle attività di trattamento rappresenta quindi uno strumento di trasparenza e rendicontazione che permette alle autorità di monitorare e verificare la conformità del trattamento dei dati personali alle disposizioni del Regolamento.

Il registro deve contenere necessariamente tutte le seguenti informazioni:

- il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o

dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1

Infine in maniera alquanto lapidaria all'articolo 31 intitolato "*Cooperazione con l'autorità di controllo*" è previsto l'obbligo generale per il titolare, il responsabile e quando previsto del loro rappresentante, di cooperare con l'autorità di controllo nell'esecuzione dei suoi compiti, qualora ne faccia richiesta.

C) Le valutazioni d'impatto

Un ulteriore onere individuato dal GDPR è stabilito dall'articolo 35 ("*Valutazione d'impatto sulla protezione dei dati*") il quale rappresenta un'importante novità introdotta dal Regolamento 2016/679.

Il primo paragrafo stabilisce che, in situazioni in cui un trattamento di dati personali, a causa dell'uso di nuove tecnologie o in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento stesso, possa comportare un rischio elevato per i diritti e le libertà delle persone interessate, il titolare del trattamento è tenuto a condurre una valutazione dell'impatto potenziale di tali operazioni preventive.

Il paragrafo 3 successivamente specifica alcune circostanze in cui questa analisi dell'impatto è particolarmente richiesta, ad esempio quando si tratta di: "*una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o*

incidono in modo analogo significativamente su dette persone fisiche"[138] oppure quando ci troviamo di fronte al "*trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1.*"[139]

E' invece il paragrafo 7 che specifica quale debba essere il contenuto minimo della valutazione d'impatto, ovvero:

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

D) Privacy by design e privacy by default

L'origine dell'espressione "*privacy by design*" può essere fatta risalire alla 32ª Conferenza Internazionale dei Garanti Privacy, ideata da Ann Cavoukian.[140] Il concetto fondamentale alla base della privacy by design è che le organizzazioni responsabili del trattamento dei dati dovrebbero considerare, sin dall'inizio dello sviluppo di qualsiasi applicazione destinata a tale trattamento, i potenziali rischi che questo comporterebbe.

Concretamente, il principio della privacy by design si traduce nell'attenzione dedicata a sette punti chiave:

- la prevenzione è preferibile alla correzione;

[138] Cfr. Art. 35 paragrafo 3 lettera a)
[139] Cfr. Art. 35 paragrafo 3 lettera b)
[140] Cavoukian, 2010

- privacy come impostazione di default, secondo cui non sta all'utente doversi preoccupare della tutela dei propri dati, dato che l'applicativo è pensato per questo;
- privacy incorporata nel progetto, ovvero il principio secondo cui lo stesso sviluppo ingegneristico dell'applicativo preposto al trattamento dei dati deve essere concepito tenendo conto dei rischi legati alla privacy degli utenti;
- massima funzionalità, ovvero il concetto secondo cui un equilibrio tra le esigenze dell'azienda che tratta i dati e il rispetto del diritto dell'interessato è possibile.
- la sicurezza deve accompagnare tutte le fasi del trattamento;
- la trasparenza, ovvero il fatto che qualsiasi modifica all'applicativo debba essere resa nota;
- la centralità dell'utente, ovvero che la privacy dell'utente non sia tutelata solo nella forma, ma anche nella sostanza.

Nel GDPR trova espressione nell'art. 25 che al paragrafo 1 statuisce: "*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati [...]*"[141]

Il principio della "*privacy by default"* invece è espresso nel secondo paragrafo dell'art. 25:

[141] Cfr. Art. 25 paragrafo 1 GDPR

"Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica."[142]

L'importanza e l'ampia portata di questi due principi non possono essere minimizzate in alcun modo. Essi impongono un approccio proattivo sia alle imprese che alle pubbliche amministrazioni. La protezione dei dati personali è ormai considerata un elemento strategico fondamentale che richiede valutazioni e considerazioni fin dalle prime fasi di progettazione di nuove procedure, prodotti o servizi.

E) Il DPO (Data Protection Officer)

Per completare l'analisi dei doveri del titolare e del responsabile del trattamento, è fondamentale dedicare un'attenzione speciale a una delle figure soggettive più rilevanti introdotte dal Regolamento 2016/679: il Responsabile della protezione dei dati, noto come Data Protection Officer (DPO), la cui normativa è dettagliata negli articoli 37, 38 e 39 del Regolamento.

Il Data Protection Officer (DPO) è una figura terza rispetto al titolare o al responsabile del trattamento che lo nomina. È un organismo designato specificamente dal GDPR con il compito di assistere il titolare/responsabile del trattamento nella vigilanza e nell'attuazione delle disposizioni del regolamento.[143] Il DPO, in conformità alla legge, svolge una funzione che

[142] Cfr. Art. 25 paragrafo 2 GDPR
[143] Cfr. Considerando 97 GDPR

abbraccia elementi di consulenza, vigilanza e controllo, operando con completa autonomia e indipendenza.[144]

Dato l'importante ruolo e le complesse responsabilità del Data Protection Officer (DPO), è essenziale che:

- Il DPO sia un professionista altamente qualificato con competenze specialistiche approfondite in materia di protezione dei dati personali, comprese la conoscenza dettagliata della normativa e delle prassi pertinenti.[145]
- Il DPO debba godere di totale indipendenza nel suo ruolo, senza conflitti di interesse che potrebbero compromettere la sua capacità di adempiere ai suoi doveri in modo obiettivo.[146]
- Il DPO sia posizionato all'interno dell'organizzazione designante in una posizione che gli consenta di riportare direttamente al più alto livello gerarchico,[147] garantendo così un canale di comunicazione efficace e diretto per la gestione delle questioni relative alla protezione dei dati.[148]

Per ciò che riguarda la sua designazione il titolare e il responsabile del trattamento, sulla base dell'Articolo 37 paragrafo 1, devono designare un DPO quando:

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

[144] Cfr. Art. 38 paragrafo 3 e 6 GDPR
[145] Cfr. Art 37 paragrafo 5 GDPR
[146] Cfr. Considerando 97 GDPR
[147] Cfr. Art 38 paragrafo 3 GDPR
[148] Cfr. Art 38 paragrafo 6 GDPR

- Il titolare o il responsabile trattano dati sensibili o dati giudiziari.

Si tratta ovviamente di casi in cui si ritiene che il trattamento presenti rischi specifici.[149]

[149] Perugini R.; "*Il Data Protection Officer: le caratteristiche e i connessi profili di responsabilità*" European Journal of Privacy Law & Tchnologies, 2019, 25ss

CAPITOLO III - L'AI ACT:

Il Parlamento europeo in data 14 giugno 2023 ha approvato il c.d. *Artificial Intelligence Act* con 499 voti a favore, 28 contrari e 93 astensioni avvicinandosi così sempre di più alla conclusione di un iter legislativo iniziato il 21 aprile 2021 con la Proposta di regolamento che stabilisce norme armonizzate sull'intelligenza artificiale da parte della Commissione europea. L'approvazione definitiva di questa regolamentazione sull'IA dovrebbe arrivare a fine anno mentre la sua entrata in vigore dovrebbe arrivare tra il 2024 e il 2025; questo perché i membri del Parlamento europeo dovranno discutere i dettagli con il Consiglio dell'Unione europea e la Commissione europea prima che i progetti di norme diventino legislazione. La legislazione finale dunque sarà presumibilmente un compromesso tra i diversi progetti delle tre istituzioni ed ecco perché probabilmente ci vorranno circa due anni prima che le leggi siano effettivamente implementate.

Nonostante dunque non abbiamo ancora una legislazione definitiva, il grado di maturità raggiunto dal processo di approvazione del regolamento europeo sull'IA ci permette di svolgere delle riflessioni approfondite sull'impatto dell'*AI Act* nel panorama europeo.

La proposta mira, nel complesso, a fornire un quadro armonizzato per lo sviluppo, la commercializzazione e l'impiego dei sistemi di IA nel rispetto dei valori, diritti e principi fondamentali dell'Unione.[150] L'AI Act, dunque, viene proposto con l'obbiettivo di non imbrigliare la ricerca e di non limitare l'imprenditoria, ma vuole dare una direzione identitaria europea rispetto all'uso della tecnologia e rispetto alle direzioni scientifiche e dell'innovazione in cui il valore della human dignity viene tutelato e preferito al valore della strategia di crescita

[150] Schneider G.; Responsabilità Civile e Previdenza, fasc.3, 1 Marzo 2023, pag. 1014

a controllo statale o della pura libertà di impresa. Nello specifico, gli obbiettivi dell'Artificial Intelligence Act sono:[151]

- assicurare che i sistemi di IA immessi sul mercato dell'Unione e utilizzati siano sicuri e rispettino tutte le normative vigenti in materia di diritti fondamentali e i valori proposti dall'Unione;
- assicurare la certezza del diritto per stimolare gli investimenti e l'innovazione nell'IA;
- 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.[152]

1. LE FONTI DEL REGOLAMENTO

Per quanto riguarda la base giuridica della proposta essa è costituita dall'*art. 114 TFUE* il quale prevede l'adozione di misure destinate ad assicurare l'instaurazione ed il funzionamento del mercato interno.[153] Tale disposizione permette di determinare vincoli uniformi e direttamente applicabili su tutto il territorio dell'Unione, con l'obbiettivo di fissare un quadro normativo omogeneo e tendenzialmente rigido per gli Stati membri, salvo taluni margini di manovra (predisposti dal regolamento) per l'organizzazione interna degli Stati e per il regime sanzionatorio.

All'esigenza di garantire all'Ue un quadro giuridico uniforme e certo si accompagna anche l'esigenza di individuare dei meccanismi di aggiornamento della disciplina; questo è dovuto al

[151] Marseglia G. "*AI Act: Impatti e Proposte. Opportunità e rischi dell'over-e under-regulation*" Article on ResearchGate, 2022, p. 21
[152] 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
[153] Art. 114 TFUE

fatto che l'IA risulta difficile da regolare, sia perché è caratterizzata da veloci ed incessanti sviluppi tecnologici che rendono obsoleta qualsiasi disciplina volta a regolarla, sia perché nei suoi sistemi più avanzati (*machine learning, deep learning*) si contraddistingue per una forte dose di autonomia e imprevedibilità la quale può rappresentare una potenziale fonte di rischi non calcolabili ex ante. Ecco che allora la Commissione tenendo conto anche di tale aspetto introduce dei meccanismi di flessibilità del quadro normativo che lo rendano, come indicato nei documenti di accompagnamento alla proposta, *future-proof:*

- In primo luogo, la proposta dell'IA Act si completa di alcuni annessi che sono fondamentali, per esempio, per individuare la categoria dei dispositivi ad alto rischio per cui si prevede una specifica procedura di verifica della conformità. Per la modifica di tali annessi si prevede sia competente la Commissione[154] affiancata dai Comitati della Comitologia.[155] Così facendo, nel caso si evidenzino problemi in relazione all'individuazione delle categorie dei sistemi ad alto rischio o alle procedure di conformità, sarà possibile apporre modifiche alla disciplina anche al di fuori del procedimento legislativo ordinario normalmente richiesto per la revisione formale del regolamento.
- In secondo luogo, all'art. 84 della Proposta è previsto che entro (tre anni dalla data di applicazione del presente regolamento di cui all'articolo 85, paragrafo 2) e successivamente ogni quattro anni, la Commissione trasmette al Parlamento europeo e al Consiglio una relazione di valutazione e sul riesame del presente regolamento. Le relazioni sono rese pubbliche.[156]

[154] Questo avviene ai sensi dell'art 290 TFUE (atti delegati)
[155] Art. 74 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
[156] Casonato C. Marchetti B.; "*Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*" in Biolaw Journal – Rivista di Biodiritto, n. 3/2021, p. 223-227

Considerando poi che la proposta contiene regole specifiche sulla protezione delle persone fisiche per quanto concerne il trattamento di dati personali, sono infatti previste particolari restrizioni sull'utilizzo dei sistemi di IA per l'identificazione biometrica remota in tempo reale in spazi accessibili al pubblico a fini di attività di contrasto, è opportuno basare il regolamento, per quanto concerne tali regole specifiche, sull'*art. 16 TFUE*.

Per ciò che concerne invece la scelta di un regolamento come atto giuridico, essa è giustificata dalla necessità di un'applicazione uniforme delle regole, inoltre l'applicabilità diretta di un regolamento[157] ridurrà la frammentazione giuridica e faciliterà lo sviluppo di un mercato unico per i sistemi di IA.

2. STRUTTURA ED ELEMENTI PRINCIPALI DEL REGOLAMENTO

Il cardine della proposta sembra risiedere nella definizione di un modello regolatorio finalizzato alla gestione ottimale dei rischi insiti nell'utilizzo dei dispositivi IA con l'obiettivo primario di tutela dei diritti fondamentali e di salvaguardia del processo democratico.[158] Questa impostazione è propria dell'approccio europeo sin dai primi documenti redatti dal Parlamento Europeo e dalla Commissione, tutti convergenti nel dare concreta attuazione alla linea giuspolitica per cui devono essere i diritti fondamentali (e il parco di valori europei che in essi si riflettono) a guidare lo sviluppo del mercato e non viceversa.[159] L'approccio utilizzato dal legislatore europeo per regolamentare l'intelligenza artificiale è di natura orizzontale. Tuttavia, questo approccio presenta una limitazione intrinseca. Siccome le norme non sono focalizzate su risolvere problemi specifici o colmare lacune specifiche nel sistema legale ma devono essere

[157] L'applicabilità diretta del regolamento è sancita dall'art 288 TFUE
[158] Floridi L.; "*The European Legislation on AI: a Brief Analysis of its Philosophical Approach"*, 34 Philosophy and Technology 215, 2021
[159] Roberts H.; "*Achieving a 'Good AI Society': Comparing the Aims and Progress of the EU and US*", 2019, p. 50

applicabili a tutti i settori, tali norme non permettono di affrontare una questione particolare o eliminare ostacoli legali specifici, ma esse, essendo di carattere generale, hanno il compito di delineare un quadro complessivo e un contesto di riferimento in cui opereranno i sistemi di intelligenza artificiale, compresi quelli che saranno sviluppati in futuro. [160]

Dal punto di vista della struttura l'AI Act è articolato in 12 titoli, che ricomprendono 85 articoli, preceduti da 89 considerando. Il testo è inoltre corredato da 9 allegati tecnici.

La prima parte della Proposta, che ricomprende il *Titolo I*, definisce l'oggetto e il campo di applicazione del Regolamento stesso. Le nuove norme sono dirette:

- ai fornitori che immettono sul mercato o mettono in servizio sistemi di IA all'interno dell'Unione;
- agli utenti di sistemi di IA situati nell'Unione;
- ad utenti e fornitori di sistemi situati in un paese terzo, quando "*l'output prodotto dal sistema sia utilizzato nell'Unione*" [161]

L'*art 3* contiene le definizioni utilizzate all'interno del documento; come ad esempio quella di "*sistema di intelligenza artificiale*" di cui si dirà più dettagliatamente nel corso di tale elaborato, oppure di "*utente*", intendendosi "*qualsiasi persona fisica o giuridica... che utilizza un sistema di IA sotto la sua autorità"* e dunque conferendogli un significato diverso rispetto a quello comune di "utilizzatore finale".

La sezione successiva della Proposta (*sezioni II-IV*) tratta la regolamentazione delle varie categorie di sistemi di intelligenza artificiale identificate dal legislatore europeo. La suddivisione adottata segue un approccio chiamato "*risk-based*", che si basa sul livello di

[160] Finocchiaro G.; Rivista Trimestrale di Diritto Pubblico, fasc.4, 1 dicembre 2022, p. 1085
[161] Art 2 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

rischio associato alle caratteristiche o all'impiego di tali tecnologie. Vengono così individuati i sistemi che comportano:

- Un rischio inaccettabile
- Un rischio alto
- Un rischio medio o basso

Il *Titolo II*, che coincide con il solo *art. 5*, disciplina le "*pratiche*" – ossia gli utilizzi o gli effetti dell'IA – qualificate come proibite nell'ordinamento comunitario, in ragione del loro patente contrasto con i valori o i diritti fondamentali dell'Unione. Il divieto riguarda queste categorie:

- le *pratiche cd. di manipolazione*, che utilizzano tecniche subliminali o altrimenti sfruttano la vulnerabilità di determinati gruppi di persone al fine di distorcerne il comportamento in modo potenzialmente dannoso;
- le *pratiche cd. di social scoring*, che utilizzano l'IA allo scopo di valutare o classificare l'affidabilità delle persone in determinati contesti sociali (ma solo, si badi, da parte di autorità pubbliche);
- l'uso di *sistemi di identificazione biometrica a distanza* (riconoscimento facciale e vocale) in tempo reale in spazi pubblicamente accessibili

Il *Titolo III* comprende le norme riguardanti i sistemi di intelligenza artificiale che comportano un rischio significativo per la salute, la sicurezza o i diritti fondamentali delle persone fisiche. Questi sistemi sono consentiti nell'ambito dell'Unione Europea purché soddisfino specifici requisiti e siano sottoposti a una valutazione preliminare di conformità prima di essere messi sul mercato o utilizzati.[162] Il *Capo 1 del Titolo III* individua i requisiti necessari affinché un sistema di IA debba essere considerato ad alto rischio:

[162] Contissa G.; Galli F.; Godano F.; Sartor G.; Rivista semestrale on-line: www.i-lex.it Dicembre 2021 Fascicolo 2

- La prima è che il sistema sia destinato a essere utilizzato come componente di sicurezza di un prodotto, o sia esso stesso un prodotto disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato II;
- La seconda che 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

Il *Capo 2* stabilisce i requisiti obbligatori per questi sistemi, ponendo particolare enfasi sulla gestione dei dati, sugli obblighi di trasparenza e sulla spiegabilità (explainability) del sistema, sulla sicurezza e la robustezza tecnica, nonché sulla necessità di supervisione umana. Nel *Capo 3* sono imposti una serie di obblighi sia ai fornitori e agli utenti che agli altri soggetti coinvolti nel ciclo di vita di tali sistemi. I *Capi 4 e 5*, invece, regolamentano gli organismi e le procedure inerenti alla valutazione di conformità anticipata a cui questi sistemi sono soggetti. Tale valutazione si basa su un modello di controllo interno all'interno delle organizzazioni e si completa con i meccanismi di verifica esterni successivi, come indicati nei *Titoli VI* e successivi. La *Sezione 5*, infine, fornisce un'analisi dettagliata delle norme relative a questi meccanismi di controllo.[163]

Il *Titolo IV* della Proposta dispone alcuni obblighi di trasparenza – diversi e ulteriori rispetto a quelli previsti per i sistemi ad alto rischio – in capo a determinati sistemi di IA che presentano specifici rischi per le persone fisiche. Si tratta di quei sistemi che

- interagiscono con gli esseri umani;

[163] Chiappini D.; Intelligenza Artificiale e responsabilità civile: nuovi orizzonti di regolamentazione alla luce dell'Artificial Intelligence Act dell'Unione europea; Fascicolo 2-2022 p. 90ss

- oppure sono utilizzati per rilevare le emozioni o determinare l'associazione con categorie (sociali) sulla base di dati biometrici;
- o ancora che generano o manipolano contenuti audiovisivi ("*deep fakes*").

In tali casi, si prevede che chi utilizza il sistema debba essere informato del fatto che sta interagendo con un'IA. I sistemi elencati corrispondono generalmente ad una tipologia di IA che viene comunemente definita "a medio rischio".

La terza parte della Proposta (*Titoli V-XII*) contiene la normativa sulla governance e sul controllo dei sistemi di IA, insieme alle regole sull'esecuzione del Regolamento.

Il *Titolo V* ha come scopo principale la creazione di un contesto giuridico che favorisca l'innovazione sia a livello tecnologico che sociale. A questo scopo, viene sostenuta l'istituzione di "*ambiti normativi controllati*" (regolamentazione sandboxes) per la sperimentazione tecnologica, fornendo un quadro normativo essenziale.

Il *Titolo VI* disciplina le istituzioni che sovrintendono al sistema di mercato dell'IA a livello sia dell'Unione Europea che degli Stati membri. In questa ottica, il legislatore europeo prevede l'istituzione di un Comitato Europeo per l'Intelligenza Artificiale, il quale avrà il compito di coordinare e supervisionare il sistema. Inoltre, vengono definite le competenze delle autorità nazionali competenti in materia.

Il *Titolo VII* mira a facilitare la governance attraverso la creazione di un archivio dati europeo dedicato ai sistemi di IA ad alto rischio.

Il *Titolo VIII* regolamenta il monitoraggio successivo all'introduzione dei sistemi di IA sul mercato, stabilisce gli obblighi informativi e prevede la vigilanza del mercato.

Nel *Titolo IX*, vengono fornite disposizioni per la creazione di codici di condotta destinati ai fornitori di sistemi di IA non ad alto rischio. Questi codici mirano a incoraggiare l'adozione volontaria, anche da parte di questi fornitori, dei requisiti vincolanti per i sistemi ad alto rischio.

Gli ultimi Titoli contengono norme di carattere generale che guidano l'attuazione futura del Regolamento: l'obbligo di riservatezza nella gestione delle informazioni da parte delle autorità pubbliche (*Titolo X*); le disposizioni relative al potere di adottare atti delegati (*Titolo XI*); gli impegni della Commissione Europea a valutare periodicamente la necessità di aggiornamenti e a preparare relazioni periodiche sulla valutazione e revisione del Regolamento (*Titolo XII*).[164]

3. LA DEFINIZIONE DI IA SECONDO L'IA ACT

La definizione di Intelligenza Artificiale contenuta nell'Articolo 3, paragrafo 1 della proposta è suddivisa in due parti. La prima parte è formulata in modo estremamente inclusivo ed include il software 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*".

La seconda parte è composta da un elenco dettagliato di tecniche e metodi che delineano chiaramente il campo di applicazione dei sistemi di IA inclusi nell'Allegato I. Questo elenco si basa su tre modelli principali: l'apprendimento automatico (che include apprendimento supervisionato e non supervisionato, oltre all'apprendimento per rinforzo), approcci basati sulla

[164] Contissa G.; Galli F.; Godano F.; Sartor G.; Rivista semestrale on-line: www.i-lex.it Dicembre 2021 Fascicolo 2

logica e modelli espliciti di conoscenza (come i sistemi esperti), e approcci statistici (come metodi di ricerca e ottimizzazione).[165]

Le due parti della definizione hanno chiaramente obiettivi diversi. La definizione generale, in linea con l'approccio basato sul rischio adottato nella Proposta, è formulata in modo neutro rispetto alla tecnologia e si concentra sulle capacità di influenza del sistema sull'ambiente circostante. D'altra parte, l'elenco delle tecniche nell'Allegato I mira a limitare l'ambito di applicazione a tecnologie specifiche, evidentemente per fornire maggiore chiarezza ai produttori e agli utilizzatori di sistemi di intelligenza artificiale.[166]

Tale definizione però suscita qualche perplessità; in particolare il riferimento ai tre approcci potrebbe condurre a comprendere anche tecnologie che normalmente non sono considerate IA; inoltre il confine tra le varie tecniche non è sempre chiaro, creando così un grado di incertezza tra gli operatori di mercato al momento di determinare se un certo sistema di IA adotti o meno le tecniche definite nell'Allegato I. D'altro canto, se la definizione di IA fosse interpretata in senso troppo stretto, potrebbe finire per escludere alcune applicazioni di sistemi automatizzati che, presentano un alto grado di rischio, specialmente quando progettati per essere indipendenti dall'intervento/supervisione umana. [167]

Questo tipo di definizione se da un lato lascia qualche perplessità circa l'identificazione precisa e netta di un'IA, dall'altro lato rispecchia come già sottolineato in precedenti passaggi di tale elaborato, la propensione a creare un Regolamento che sia in grado di adattarsi alla costante evoluzione tecnologica in atto nel nostro mondo. Tenendo a mente tale aspetto si comprende

[165] A tal proposito è da sottolineare come nell'articolo 4 della Proposta si stabilisce l'uso di atti delegati per modificare l'elenco delle tecniche e degli approcci definiti nell'allegato I per mantenere l'elenco aggiornato agli sviluppi futuri del mercato e delle tecnologie
[166] Contissa G.; Galli F.; Godano F.; Sartor G.; Rivista semestrale on-line: www.i-lex.it Dicembre 2021 Fascicolo 2
[167] Dignum V.; "*Responsible artificial intelligence: how to develop and use AI in a responsible way*", Springer Nature, 2019, p. 120

anche la disposizione dell'art. 4 del Regolamento che consente alla Commissione di modificare l'Allegato I adattando flessibilmente l'ambito di applicazione del quadro normativo;[168] Lo stesso Libro bianco sull'IA sottolinea "*qualunque nuovo strumento giuridico dovrà comprendere una definizione di IA abbastanza flessibile da accogliere il progresso tecnico, ma anche sufficientemente precisa da garantire la necessaria certezza del diritto".*[169]

Alla luce di questo è evidente come il compromesso adottato dal legislatore europeo nella definizione di intelligenza artificiale sia un compromesso operato nella consapevolezza della peculiarità del fenomeno trattato; così il corretto bilanciamento tra certezza giuridica e flessibilità della definizione è stato individuato come l'unico modo per permettere all'AI Act di resistere al progresso tecnologico.[170]

4. LE PRATICHE DI INTELLIGENZA ARTIFICIALE VIETATE

Il Titolo II della Proposta contiene soltanto l'articolo 5 il quale si occupa di alcune pratiche realizzate attraverso sistemi di intelligenza artificiale che generano o possono generare effetti inaccettabili poiché in contrasto con i valori e i diritti fondamentali dell'Unione. Salvo alcune eccezioni la Proposta pone un divieto generalizzato. Di seguito l'analisi di queste pratiche vietate.

A) Manipolazione

L'articolo 5 (1) lett. a, proibisce "*l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che utilizza tecniche subliminali che agiscono senza che una persona ne sia*

[168] Cfr. Art 4 AI Act
[169] Cfr. Libro bianco sull'intelligenza artificiale
[170] Fidanza F.; "*Sul concetto di intelligenza artificiale*", La Nuova Giuridica, 1/2022

consapevole al fine di distorcerne materialmente il comportamento in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico".

Prima di tutto è opportuno analizzare alcuni termini di tale disposizione per comprendere il significato che l'AI Act attribuisce a certi termini; in particolare i concetti di "*immissione sul mercato" e "messa in servizio*".

Per quanto riguarda *l'"immissione sul mercato"* di un sistema di IA la proposta intende "*la prima messa a disposizione di un sistema di IA sul mercato dell'Unione*"[171] e la "*messa a disposizione sul mercato"* è a sua volta definita come "*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*"[172]

La "*messa in servizio"* di un sistema di IA è definita invece come "*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*"; si intende poi per "*finalità prevista"* l'uso di un sistema di IA previsto dal fornitore, compresi il contesto e le condizioni d'uso specifici, come dettagliati nelle informazioni comunicate dal fornitore nelle istruzioni per l'uso, nel materiale promozionale o di vendita e nelle dichiarazioni, nonché nella documentazione tecnica.

Fatta questa analisi necessaria, se si analizza la versione definitiva dell'art 5 (1) lett. A con quella precedente della Proposta si nota che ora le restrizioni sulla manipolazione sembrano più precise sia nella loro struttura che nei loro effetti. In termini di struttura, la manipolazione non è più definita in base all'architettura o all'interfaccia digitale,[173] ma piuttosto in termini di

[171] Cfr. Art. 3 n. 9 AI Act
[172] Cfr. Art. 3 n. 10
[173] L'art. 4 della versione non ufficiale recitava "*AI systems designed or used in a manner that manipulates human behaviour, opinions or decisions through choice architectures or other elements of user interfaces, causing a person to behave, form an opinion or take a decision to their detriment.*"

un'azione specifica: il ricorso a tecniche subliminali al di fuori della consapevolezza di una persona.[174]

Nonostante la nuova formulazione del divieto sia più specifica, lascia aperte alcune questioni importanti. Innanzitutto non è chiaro il significato delle "*tecniche subliminali*", successivamente l'interpretazione della "*consapevolezza*" in relazione alle pratiche che si svolgono al di fuori di essa non è del tutto comprensibile. Come se ciò non bastasse per quanto riguarda il risultato della manipolazione, le tipologie di danno menzionate nel divieto risultano poco chiare. Mentre il danno fisico è teoricamente più facile da individuare, identificare il danno psicologico è complesso a causa della sua intrinseca soggettività e della mancanza di indicatori chiari e metodi di misurazione. La formulazione vaga potrebbe portare a considerare dannosi dal punto di vista psicologico anche gli annunci mirati sulle piattaforme digitali, ogni volta che una persona prova fastidio o irritazione a causa dell'intrusione nella propria sfera privata.

Il rischio è dunque che il divieto di manipolazione, pur se maggiormente dettagliato rispetto alla bozza iniziale, sia comunque concretamente difficile da provare a causa di una certa indeterminatezza circa le pratiche o tecniche che siano considerate effettivamente così pericolose da mettere in pericolo gli individui.[175]

B) Sfruttamento di gruppi vulnerabili

La seconda pratica vietata è indicata all'art 5 (1) lett. B: "*l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che sfrutta le vulnerabilità di uno specifico gruppo di*

[174] Orlando S.; "*Regole di immissione sul mercato e pratiche di intelligenza artificiale vietate nella Proposta di Artificial Intelligence Act*" in "*Persona e Mercato*" 2022/3 p. 346 ss
[175] Contissa G.; Galli F.; Godano F.; Sartor G.; Rivista semestrale on-line: www.i-lex.it Dicembre 2021 Fascicolo 2

persone, dovute all'età o alla disabilità fisica o mentale, al fine di distorcere materialmente il comportamento di una persona che appartiene a tale gruppo in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico"

L'attenzione ai gruppi più deboli assume certamente un valore etico molto importante; tuttavia anche questa disposizione presenta qualche problematica. Innanzitutto non viene specificato cosa si intenda per "*sfruttamento";* in questo contesto, si potrebbe considerare che lo sfruttamento sia una pratica diversa rispetto alla manipolazione, e che l'utilizzo delle informazioni possa condurre a considerare alcune persone fisiche come vulnerabili. Ad esempio, un sistema che sfrutta le informazioni sull'età di una persona per promuovere l'acquisto di prodotti per bambini sembrerebbe rientrare nell'ambito di applicazione di questa disposizione.[176] Inoltre, per quanto riguarda l'approccio concettuale alla vulnerabilità, si fa riferimento a gruppi che, a causa di specifiche caratteristiche come l'età e la disabilità fisica o mentale, sono tradizionalmente considerati più vulnerabili.[177] Non è chiaro perché solo questi tipi di vulnerabilità siano prese in considerazione e non anche altre, come ad esempio vulnerabilità in ambito finanziario o di marketing sempre più presenti e pressanti nel mondo attuale.

In conclusione, è possibile argomentare che quando si tratta di sistemi di intelligenza artificiale, la vulnerabilità è intrinseca e può potenzialmente coinvolgere chiunque. Questo tipo di

[176] Casonato C., Marchetti B.; "*Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*" in BioLaw Journal – Rivista di BioDiritto, n. 3/2021

[177] Il Regolamento sembra seguire attentamente la Direttiva 2005/29/CE sulle pratiche commerciali scorrette, la quale stabilisce che le pratiche commerciali che possono influenzare negativamente un gruppo di consumatori vulnerabili a causa della loro infermità mentale o fisica, età o ingenuità, e se questa vulnerabilità è ragionevolmente prevedibile dal professionista, devono essere valutate considerando il comportamento medio del consumatore.

vulnerabilità non deriva dalle caratteristiche personali o dalle circostanze individuali, ma è insita nel sistema di intelligenza artificiale con cui le persone interagiscono[178]

C) Social scoring pubblico

Il terzo divieto si riferisce ai sistemi di intelligenza artificiale destinati al cosiddetto "*social scoring*", che implica la valutazione e la classificazione dell'affidabilità delle persone in base al loro comportamento in contesti sociali specifici o ad altre caratteristiche personali.

La norma vieta la vendita e l'uso di tali sistemi da parte delle autorità pubbliche o di terzi che agiscono per conto delle autorità pubbliche, quando il social scoring comporta un trattamento dannoso o svantaggioso per individui o gruppi di persone. Questo divieto si applica in due situazioni:

- quando l'effetto dannoso si verifica in contesti sociali diversi da quelli in cui i dati utilizzati dal sistema sono stati originariamente generati o raccolti;
- quando tale danno è ingiustificato o sproporzionato rispetto al comportamento sociale o alla sua gravità.[179]

La proibizione sembra essere fortemente influenzata dall'obiettivo di contrastare i sistemi di social scoring, che sono stati adottati in varia misura in paesi asiatici altamente tecnologici, come la Cina.[180] Tuttavia, sembra che il legislatore europeo abbia trascurato l'uso di sistemi di scoring da parte di entità private, che è più comune in Europa. Questa lacuna è particolarmente problematica perché anche il social scoring privato può avere un impatto significativo sui diritti

[178] Burr, C., Cristianini, N., Ladyman, J., "*An Analysis of the Interaction Between Intelligent Software Agents and Human Users*", Minds and Machines, 28, 2018, p. 735-774
[179] Cfr. Art 5 (1) lett. C AI Act
[180] Citino Y. M.; "*Social scoring e città distopica: la profilazione del cittadino con finalità di policy urbana alla prova dei valori costituzionali*" in "*La città come istituzione, entro e oltre lo Stato*" a cura di Allegri G., Frosina L., Guerra A., Longo A.; p 117ss

fondamentali e sui principi democratici fondamentali. Ad esempio, può influenzare l'accesso ai servizi essenziali come forniture di gas e acqua, servizi finanziari o assicurativi, nonché la possibilità di accedere ai servizi online per il tempo libero.[181]

D) Identificazione biometrica remota e in tempo reale

Le ultime pratiche vietate disciplinate riguardano "*l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto*"[182] [183]
In linea di massima, i sistemi di identificazione biometrica a distanza in tempo reale, come il riconoscimento facciale e vocale, sono vietati. Tuttavia, sono previste diverse eccezioni, alcune delle quali si applicano in particolare all'uso dell'intelligenza artificiale nel contesto della giustizia penale, con un focus su:

- La ricerca mirata di vittime specifiche di reati, inclusi casi di bambini scomparsi.
- La prevenzione di una minaccia specifica, sostanziale e imminente alla vita o all'incolumità delle persone o di un potenziale attentato terroristico.
- L'individuazione, la localizzazione, l'identificazione o il perseguimento di autori o sospetti di una serie specifica di reati.[184]

Negi scenari sopra menzionati, l'adozione di sistemi di identificazione biometrica a distanza in tempo reale è soggetta a specifiche garanzie procedurali. Queste garanzie includono, da un lato, una valutazione dei presupposti che autorizzano l'uso di tali tecnologie e delle possibili implicazioni per i diritti e le libertà delle persone coinvolte. Dall'altro lato, sono imposte

[181] A. Raz., Minari J.; "*Ai-driven risk scores: shoul social scoring and polygenic scores based on etnicity be equally prohibited*" Edited by Manuel Corpas, University of Westminster, United Kingdom 30 maggio 2023, p. 20ss
[182] Cfr. Art. 5 (1) lett. D
[183] Cfr. Art. 3 n.37; Tali sistemi sono definiti come sistemi "*in cui la cattura dei dati biometrici, il confronto e l'identificazione avvengono senza un ritardo significativo*". La definizione è intesa a coprire non solo l'identificazione istantanea, ma anche quella effettuata a breve distanza di tempo
[184] Cfr. Art. 5 (1) lett. D

restrizioni in termini di tempistiche, geografia e soggetti coinvolti nell'uso di questi sistemi. In tutti i casi, è richiesta un'autorizzazione preventiva da parte dell'autorità giudiziaria o di un'autorità amministrativa indipendente del rispettivo Stato membro, che viene concessa solo su richiesta motivata.

Tuttavia, in situazioni di urgenza adeguatamente giustificate, l'autorizzazione può essere richiesta durante o dopo l'uso del sistema. L'autorità competente può concedere questa autorizzazione solo se è dimostrato, sulla base di prove oggettive o chiare indicazioni fornite, che l'uso del sistema in questione è necessario e proporzionato per raggiungere uno dei fini consentiti dalla Proposta.[185]

Considerando l'alto grado di rischio associato a questi sistemi, è positivo che si stia affrontando una regolamentazione dettagliata per i sistemi di identificazione biometrica. Tuttavia, è importante notare che la portata delle disposizioni appare limitata e, allo stesso tempo, ambigua.

La proibizione dei sistemi biometrici si applica solo all'"*identificazione*" delle persone fisiche. Tuttavia, il termine "identificazione" non è sempre sufficiente per descrivere appieno le caratteristiche di queste tecnologie. È noto che molti dei sistemi che utilizzano dati biometrici, come il monitoraggio dei movimenti degli occhi e delle labbra, la frequenza cardiaca o la conduttanza cutanea, non hanno l'obiettivo di identificare un individuo specifico (cioè associare una persona fisica a un nome e un cognome). Invece, sono utilizzati per il "*riconoscimento*" degli individui, categorizzandoli in classi o metriche predefinite e valutando il loro comportamento, che può essere considerato pericoloso o indesiderabile. La formulazione

[185] Lavorgna, A., Suffia, G.; "*La nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale e la sua rilevanza nell'ambito della giustizia penale: un passo necessario, ma non sufficiente, nella giusta direzione*", Diritto Penale Contemporaneo, 2021, pp. 88-103

attuale dunque potrebbe causare grossi dubbi e problemi interpretativi al momento dell'applicazione pratica della norma.[186]

5. Sistemi IA ad alto rischio

In coerenza con l'approccio basato sulla gestione del rischio scelto, l'uso e lo sviluppo di "*sistemi di intelligenza artificiale ad alto rischio*" sono consentiti sul mercato europeo a condizione che vengano rispettati determinati requisiti obbligatori e che sia condotta un'adeguata valutazione di conformità anticipata. La classificazione di un sistema di intelligenza artificiale come ad alto rischio non dipende unicamente dalla sua funzione, ma anche dalla finalità specifica e dalle modalità con cui viene utilizzato.[187]

Analogamente alla definizione di IA, la determinazione dell'alto rischio è suddivisa in due parti; innanzitutto, si precisa come possano essere considerati ad alto rischio sia i singoli dispositivi di IA che possano incidere sui diritti fondamentali, sia i sistemi che costituiscono una componente di sicurezza di un prodotto (o di una sua parte) soggetti a regolamentazione nell'ambito del *New Legislative Framework* (NFL).[188] Le normative di riferimento sono elencate nell'allegato II e comprendono, tra le altre, la direttiva 2009/48/CE sulla sicurezza dei giocattoli e il Regolamento (UE) 2017/745 sui dispositivi medici. La seconda parte della definizione di alto rischio consiste anche in questo caso in un elenco. Questo elenco è dettagliato nell'Allegato III e comprende otto macroaree in cui i sistemi di IA utilizzati sono presumibilmente a alto rischio. Tra queste macroaree figurano l'identificazione biometrica,

[186] Raffiotta E., C., Baroni M.; "*Intelligenza artificiale, strumenti di identificazione e tutela dell'identità*" BioLaw, 12 aprile 2022, p. 165-172
[187] Chiappini D.; "*Intelligenza Artificiale e responsabilità civile: nuovi orizzonti di regolamentazione*" Rivista italiana di informatica e diritto, Fascicolo 2-2022, p. 90ss
[188] Cfr. Art 6 Ai Act

l'accesso a servizi pubblici e privati, le attività di contrasto e l'amministrazione della giustizia.[189]

I sistemi inclusi in queste categorie devono rispettare una serie rigorosa di regole che si applicano a sviluppatori, fornitori e utenti. Queste regole comprendono la creazione di un sistema di addestramento e validazione (articolo 9), un obbligo di qualità e accuratezza dei dati (articolo 10), nonché l'obbligo di fornire documentazione tecnica e garantire requisiti di trasparenza verso l'utilizzatore (articolo 13).[190]

La maggior parte degli obblighi ricadono sul fornitore, ovvero la persona o ente che sviluppa un sistema di IA ad alto rischio per immetterlo sul mercato.[191]

In generale, i fornitori di sistemi di IA ad alto rischio devono implementare un sistema di gestione della qualità che assicuri la conformità a una serie di requisiti. Tra questi requisiti rientrano una governance adeguata dei dati (articolo 10), la fornitura di informazioni trasparenti agli utenti (articolo 13) e la supervisione umana (art. 14).

A) Dati e governance dei dati

In base all'articolo 10 *(Dati e governance dei dati),* i sistemi di IA ad alto rischio che si basano su tecniche di apprendimento dai dati devono rispettare specifici criteri di qualità; infatti essi devono essere pertinenti e rappresentativi, considerando anche le caratteristiche specifiche dell'area geografica di utilizzo. Inoltre, in modo ambizioso, il legislatore dell'UE richiede che i

[189] Cfr. Allegato III AI Act
[190] De Matos Pinto I.; "*The draft AI Act: a success story of strengthening Parliament's right of legislative initiative?*" ERA Forum, 2021
[191] Tali obblighi sono individuati dal Titolo III Capo II AI Act

dati siano privi di errori e completi, cosa che risulta particolarmente difficile da porre sempre in atto da un punto di vista tecnico.

Un'altra pratica essenziale nella governance dei dati è il monitoraggio, la rilevazione e la correzione delle distorsioni (bias). È ormai ben noto che l'uso di sistemi di intelligenza artificiale basati sull'apprendimento automatico aumenta il rischio di discriminazione indiretta, anche se non intenzionale. Questo può verificarsi in molteplici modi, a seconda di come vengono definite le variabili target del modello, di come vengono selezionate le caratteristiche del modello di apprendimento e degli elementi sostitutivi.[192]

L'ultimo comma dell'art 10 richiede poi adeguate pratiche di governance dei dati anche per sistemi di intelligenza artificiale ad alto rischio che non fanno affidamento sull'addestramento automatico.

B) Trasparenza e fornitura di informazioni agli utenti

Uno dei principali e più noti problemi che i sistemi avanzati di IA presentano riguarda la cd. *black box*. Si tratta del fatto che dispositivi capaci di machine o deep learning o che utilizzano reti neurali, sono caratterizzati da una estrema complessità che rende praticamente impossibile tracciare la catena dei passaggi seguiti per generare il risultato finale. Se l'input e l'output del processo sono noti non lo è, a motivo della sostanziale opacità delle dinamiche interne allo stesso, l'iter che ha generato la decisione né le modifiche che il dispositivo ha autonomamente assunto per raggiungere con maggior efficacia il compito assegnato.[193]

Ecco che per cercare il più possibile di ovviare tale problema l'Ai Act stabilisce che i sistemi di intelligenza artificiale ad alto rischio devono essere progettati in modo tale che le persone

[192] Barocas, A. D. Selbst, "*Big data's disparate impact*", Calif. L. Rev., 2021, p. 683.
[193] Pasquale F.; "*The Black Box Society. The Secret Algorithms That Control Money and Information*", 2015.

che li utilizzano e chi li ha creati possano capire come funzionano.[194] Devono essere fornite istruzioni chiare sulle finalità del sistema e su come controllarlo da parte delle persone.[195]

È importante notare che quando si parla di "*trasparenza*" in questa parte della proposta, si intende che gli utenti professionisti devono essere in grado di capire come funziona il sistema e quali risultati produce.

Tuttavia, ci sono alcune preoccupazioni. L'obbligo di trasparenza per i sistemi ad alto rischio potrebbe richiedere la comprensione di informazioni tecniche, il che potrebbe essere difficile per molte persone nella catena di utilizzo di prodotti o servizi di IA, che potrebbero non avere competenze tecniche. Ad esempio, pensiamo alle aziende che utilizzano sistemi di intelligenza artificiale di Google per la pubblicità mirata.

Inoltre, la descrizione dei requisiti è vaga e alcune questioni rimangono aperte. L'articolo 13 si concentra sull'interpretabilità dell'output dei sistemi di IA senza definire chiaramente cosa si intenda per "*interpretabilità*" e come sia correlata alla "*spiegabilità*".

Nel Considerando 70 della proposta, si richiede la trasparenza verso il pubblico per i sistemi ad alto rischio; tuttavia, nel testo del Regolamento non si trova un obbligo generale di trasparenza o spiegabilità nei confronti delle persone che utilizzano i sistemi. Questo rappresenta una perdita rispetto alle linee guida etiche del Gruppo di esperti sull'intelligenza artificiale, che mettevano l'accento sulla trasparenza e la spiegabilità per il pubblico. La trasparenza e la spiegabilità sono importanti perché permettono alle persone di capire perché

[194] L'art 13 parla di utenti inteso, come specificato dallo stesso Regolamento all'art 3, come "*Qualsiasi persona fisica o giuridica, autorità pubblica, agenzia o altro organismo che utilizza un sistema di IA sotto la sua autorità"*. Questa definizione si discosta da quella usata nel linguaggio comune: in questo caso l'utente non comprende l'utilizzatore finale, ossia colui che interagisce con il sistema predisposto da altri, senza avere autorità o controllo su di esso

[195] Cfr. Art 13 AI Act

un algoritmo ha preso una certa decisione e se possono accettarla o contestarla. La proposta di Regolamento sembra invece concentrarsi sulla trasparenza verso i produttori e fornitori.[196]

C) Supervisione umana

All'art. 14, la Proposta stabilisce che i sistemi ad alto rischio siano sviluppati "*anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche*". La sorveglianza, che mira a prevenire o minimizzare i rischi per la salute, la sicurezza, o i diritti fondamentali (art 14 (2)), deve essere garantita mediante misure individuate dal fornitore, e integrate nel sistema dal fornitore stesso o implementate dall'utente. Tali misure mirano a supportare le azioni indicate al paragrafo 4 dell'art. 14:

- comprendere appieno le capacità e i limiti del sistema di IA ed essere in grado di monitorarne il funzionamento;
- mantenere un atteggiamento consapevole rispetto al rischio di bias;
- essere in grado di interpretare correttamente l'output del sistema;
- essere in grado di decidere di non usare il sistema o di ignorare, annullare, o ribaltare il suo output;
- essere in grado di intervenire sul funzionamento del sistema o di interromperlo mediante un pulsante di "arresto" o una procedura analoga.

Il problema fondamentale qui è che c'è una discrepanza tra le competenze umane e le responsabilità assegnate. I sistemi di intelligenza artificiale vengono utilizzati perché sono in grado di prendere decisioni e fare previsioni in modo superiore rispetto agli esseri umani.

[196] Guidotti R.; "*A survey of methods for explaining black box models*", ACM computing surveys (CSUR), 2022, p. 15ss

Tuttavia, sono proprio gli esseri umani a dover valutare la qualità di questi sistemi, il che può creare una situazione difficile.

Anche quando gli esseri umani mantengono il controllo formale sulla decisione finale, è probabile che si affidino alle decisioni del sistema di intelligenza artificiale, soprattutto se il sistema è stato certificato. Questo accade a meno che non ci siano motivi specifici per ritenere che il sistema non funzioni correttamente o che debba tener conto di ulteriori informazioni esterne nella sua valutazione.[197]

6. SISTEMI IA A BASSO RISCHIO

Accanto ai sistemi vietati e a quelli ad alto rischio, la proposta di regolamento stabilisce una disciplina anche per i "*sistemi a basso o minimo rischio*", regolati dall'articolo 52 della proposta di regolamento. Questa categoria di intelligenza artificiale è residuale e si identifica per esclusione: sono sistemi a basso o minimo rischio tutti quelli che non rientrano né nella categoria dei sistemi vietati né in quella dei sistemi ad alto rischio. Questi sistemi costituiscono la parte più ampia delle applicazioni di IA all'interno del mercato comune europeo. La loro circolazione nell'Unione europea è libera, a meno che, a causa delle loro caratteristiche, non debbano essere imposti obblighi di trasparenza al fornitore. Questa situazione si applica in particolare ai sistemi che interagiscono con le persone (come i chatbot) e in cui la loro natura artificiale potrebbe non essere evidente a causa del contesto in cui operano. Si applica anche ai sistemi che modificano o sovrappongono immagini, video o audio per rendere autentici oggetti o persone che non lo sono realmente (noti come deepfake). In tali casi, le persone devono essere informate che è stata apportata una manipolazione artificiale ai contenuti originali in modo che non vi siano dubbi sulla loro autenticità. È possibile derogare da questi obblighi di trasparenza

[197] Chiappini D.; "*Intelligenza Artificiale e responsabilità civile: nuovi orizzonti di regolamentazione*" Rivista italiana di informatica e diritto, Fascicolo 2-2022

solo quando il sistema è autorizzato dalla legge per scopi di prevenzione e persecuzione dei reati o quando è utilizzato per garantire le libertà di espressione, artistiche o scientifiche protette dalla Carta dei diritti fondamentali dell'Unione europea. [198]

7. Valutazione di conformità, monitoraggio e il ruolo delle autorità pubbliche

Come sottolineato nei paragrafi precedenti l'immissione nel mercato di sistemi di IA ad alto rischio è condizionato al rispetto dei requisiti fissati nel capitolo II della Proposta. La Commissione per tale verifica, consentendo così la circolazione di tali prodotti nell'Unione Europea, ha optato per utilizzare il modello della procedura di marchio di conformità europea (marchiatura CE). Questa procedura è stata precedentemente utilizzata per regolare vari prodotti sul mercato europeo, come i giocattoli secondo la direttiva 2009/48 sulla sicurezza dei giocattoli e i prodotti in generale secondo la direttiva 2001/95 sulla sicurezza generale dei prodotti.

Con questa procedura, un prodotto può essere messo in circolazione nel mercato europeo solo dopo aver ottenuto il marchio di conformità. Questo marchio può essere apposto solo dopo che il produttore o un organismo di certificazione terzo ha effettuato una procedura di verifica per assicurarsi che il prodotto soddisfi gli standard e le regole stabiliti dall'Unione Europea. Dunque diversamente da quanto stabilito per l'immissione nel mercato Ue dei medicinali (dir. 2001/83 per la procedura decentrata e reg. 726/2004 per la procedura accentrata) o dei prodotti OGM (reg. 1829/2003), per i quali pure la componente di rischio è significativa, non si prevede il rilascio di un'autorizzazione pubblica, nazionale o europea, ma il rispetto dei requisiti posti a protezione della sicurezza, della salute e dei diritti fondamentali dei cittadini è garantita da un'auto-valutazione da parte del soggetto che ha interesse a commercializzare il prodotto.

[198] Casonato C., Marchetti B.; "*Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*" in BioLaw Journal- rivista di BioDiritto, n. 4/2021, p. 90ss

Questa scelta regolatoria comporta chiari vantaggi immediati: mentre l'autorizzazione pubblica offre maggiore certezza e sicurezza per quanto riguarda le verifiche sulla sicurezza dei prodotti, essa comporta anche costi significativi in termini amministrativi ed efficienza. D'altra parte, la procedura di marchio di conformità europea sposta il peso dei controlli sul produttore, semplificando l'ingresso del prodotto sul mercato e trasferendo agli operatori economici la responsabilità di garantire il rispetto dei requisiti di sicurezza stabiliti dalla normativa.[199] La scelta di questa procedura più "leggera", tuttavia, presenta un importante temperamento. Infatti, per alcuni sistemi di IA, in particolare quelli biometrici elencati nell'Allegato III, punto 1, la procedura di conformità deve essere condotta da organismi terzi, come stabilito nell'articolo 43, paragrafo 1, della Proposta. Inoltre, è importante sottolineare che, come già evidenziato riguardo alla flessibilità della regolamentazione dell'AI Act, gli stessi Allegati VI e VII, che riguardano la procedura interna o esterna di verifica di conformità, possono essere facilmente soggetti a revisione nel caso in cui il sistema non rispetti adeguatamente i requisiti.[200]

L'iniziale processo di verifica della conformità non rappresenta l'unico punto di controllo dei rischi. La proposta della Commissione prevede, infatti, un sistema di monitoraggio successivo all'ingresso nel mercato, il cui scopo è assicurare che il prodotto continui a soddisfare i requisiti stabiliti dalla regolamentazione per l'intera durata del ciclo di vita dei sistemi di IA.[201] A tale scopo, da un lato, si richiede a ciascun Stato membro di istituire un'autorità responsabile della gestione del sistema di monitoraggio post-vendita, dall'altro lato vengono stabiliti chiari obblighi sia per gli utilizzatori dei sistemi, sia per chi li fornisce. Nel caso del fornitore egli deve conservare accuratamente le registrazioni delle operazioni del sistema di IA per un

[199] Casonato C., Marchetti B.; "*Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*" in BioLaw Journal- rivista di BioDiritto, n. 4/2021, p. 90ss

[200] Mokander J.; "*Conformity assessments and post-market monitoring: a guide to the role of auditing in the proposed European AI Regulation*", Minds and Machines, 2021, p. 1-28

[201] Cfr. Art 61 Ai Act

periodo di tempo adeguato, che varia in base alle caratteristiche specifiche del sistema. Queste registrazioni possono essere accessibili alle autorità nazionali competenti per scopi di controllo. Inoltre, il fornitore è tenuto a prendere immediatamente le misure necessarie per correggere eventuali problemi e a segnalare qualsiasi violazione nel funzionamento del sistema all'autorità nazionale competente, nonché, se del caso, all'organismo di certificazione.[202]

Le regole riguardanti gli organismi certificatori e i requisiti che devono soddisfare per poter certificare la conformità dei sistemi seguono un modello simile a quello utilizzato in altre normative che riguardano il marchio di conformità comunitario.[203] In dettaglio, ogni Stato membro ha il compito di nominare un'autorità di notifica responsabile per stabilire e gestire le procedure necessarie per valutare e notificare gli organismi certificatori.[204] Questa autorità di notifica deve operare in modo tale da evitare qualsiasi conflitto di interesse con gli stessi organismi certificatori.

L'articolo 33 stabilisce in modo dettagliato i requisiti strutturali che un organismo certificatore deve soddisfare per svolgere i propri compiti. Questo organismo deve avere a disposizione risorse organizzative e finanziarie adeguate per condurre la valutazione di conformità ed è soprattutto fondamentale che sia indipendente dal fornitore del sistema ad alto rischio che sta valutando. Questa indipendenza deve essere mantenuta anche da qualsiasi altro soggetto che abbia un interesse economico nell'applicazione in esame, e deve essere garantita rispetto ai potenziali concorrenti del fornitore. L'autorità di notifica nazionale condivide con la Commissione e gli altri Stati membri un elenco degli organismi di valutazione della conformità tramite uno strumento elettronico di notifica sviluppato e gestito dalla Commissione stessa. Se sorgono dubbi sulla conformità degli organismi di verifica ai requisiti stabiliti nel regolamento

[202] Cfr. Art 20-23 Ai Act
[203] Cfr. la disciplina stabilita sugli organismi notificati e sulle autorità di notifica prevista nella direttiva 2009/48 sulla sicurezza dei giocattoli (agli artt. 22 e ss.)
[204] Cfr. Art 30 Ai Act

la Commissione ha il potere di condurre indagini e verifiche per adottare misure correttive, incluso il revocare la notifica se necessario.[205]

Gli organismi certificatori devono collaborare pienamente con l'autorità di notifica durante tutto il periodo in cui svolgono le loro attività. Devono fornire tutta la documentazione necessaria dal fornitore in modo che l'autorità possa condurre verifiche, monitorare e sorvegliare i processi per garantire che tutto sia svolto correttamente. Inoltre, hanno obblighi significativi di comunicazione, sia verso l'autorità di notifica che verso altri organismi certificatori. Gli Stati membri devono assicurare che chiunque abbia un interesse legittimo possa richiedere una revisione delle decisioni prese dagli organismi certificatori.[206] [207]

8. Intelligenza artificiale e responsabilità civile

Il percorso per creare un quadro normativo sulla responsabilità civile nell'ambito dell'Intelligenza Artificiale ha avuto inizio nel 2016, quando la commissione JURI del Parlamento europeo ha redatto un primo progetto di relazione dopo aver ascoltato numerosi esperti in campo di IA. In seguito a questa relazione[208] il Parlamento europeo ha adottato una Risoluzione il 16 febbraio 2017 mediante la quale ha raccomandato alla Commissione l'adozione di norme di diritto civile sulla robotica, includendo l'Intelligenza Artificiale.

In questa risoluzione, il Parlamento europeo ha sottolineato l'importanza della responsabilità civile per i danni causati da robot (con il termine "robot" inteso in senso ampio, che comprende l'Intelligenza Artificiale). Ha auspicato un'analisi a livello dell'Unione Europea per garantire

[205] Cfr. Art 37 Ai Act
[206] Cfr. Art. 45 Ai Act
[207] Mokander J.; "*Conformity assessments and post-market monitoring: a guide to the role of auditing in the proposed European AI Regulation*", Minds and Machines, 2021, p. 1-28
[208] Commissione JURI del Parlamento europeo, *Progetto di relazione recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*, 2016.

coerenza, efficienza e trasparenza nell'applicazione delle leggi, nell'interesse sia dei cittadini e dei consumatori che delle imprese.[209]

Già in questa risoluzione, si chiedeva alla Commissione di presentare una proposta legislativa sulle questioni giuridiche legate allo sviluppo e all'uso della robotica e dell'Intelligenza Artificiale, insieme a strumenti non legislativi come linee guida e codici di condotta.

In seguito alla Risoluzione, la Commissione europea ha intrapreso un'azione focalizzata su come adattare le norme sulla responsabilità civile per affrontare le esigenze dell'economia digitale.[210] La Commissione ha espresso l'intenzione di lavorare in collaborazione con il Parlamento europeo e gli Stati membri per sviluppare una risposta comune dell'Unione Europea a questa sfida.

Nel documento, la Commissione ha ritenuto che la "*Direttiva sulla responsabilità dei danni da prodotto difettoso*" sia strettamente correlata agli argomenti in discussione.[211] Si è dichiarato che sarà effettuata una valutazione della Direttiva al fine di determinare se e in che misura sia in grado di soddisfare gli obiettivi di garantire la responsabilità del produttore per i danni causati da prodotti difettosi, anche nel contesto dei danni provocati dalle nuove tecnologie. [212]

In parallelo al processo istituzionale, si è sviluppato un dibattito significativo sulla questione che ha riguardato sia la regolamentazione della responsabilità civile che la possibile creazione di una nuova forma di personalità giuridica. In particolare, per quanto riguarda quest'ultima, si è notato che l'applicazione dei tradizionali strumenti giuridici alle conseguenze dell'uso dei

[209] Cfr art 49 Risoluzione del Parlamento europeo; Testi approvati - Norme di diritto civile sulla robotica - Giovedì 16 febbraio 2017 (europa.eu)
[210] Cfr. Risposta della Commissione europea alla Risoluzione Norme di diritto civile sulla robotica del 16 febbraio 2017
[211] Cfr. Direttiva 85/374/CEE del 25 luglio 1985 in materia di responsabilità per danno da prodotti difettosi.
[212] Chiappini D.; "*Intelligenza Artificiale e responsabilità civile: nuovi orizzonti di regolamentazione alla luce dell'Artificial Intelligence Act dell'Unione europea*" in Rivista italiana di informatica e diritto, fascicolo 2-2022

sistemi di Intelligenza Artificiale potrebbe comportare il rischio di far ricadere il danno sulle persone danneggiate o sulla società nel suo complesso, rendendo l'uso dell'IA un rischio collettivo. Di conseguenza, la possibile soluzione a questa sfida potrebbe essere la creazione di una personalità giuridica appositamente per i sistemi di Intelligenza Artificiale. Tuttavia, questa questione è ancora aperta e oggetto di dibattito. Dal punto di vista pratico, il diritto può conferire soggettività legale a diverse entità attraverso il ricorso a concetti giuridici fittizi, come avviene per le persone giuridiche o come è stato fatto in passato per altre forme di soggettività legale. Tuttavia, questa idea è stata criticata da diverse parti o considerata intrinsecamente rischiosa, in quanto l'attribuzione di responsabilità morale può risultare problematica data la differenza tra i processi decisionali umani e quelli artificiali. Nonostante le obiezioni sollevate da coloro che sostengono questa posizione, la creazione di una forma di personalità giuridica limitata sembra essere una soluzione preferibile al fine di consentire una regolamentazione completa che possa anche anticipare eventuali sviluppi futuri nella tecnologia.[213] Le istituzioni dell'Unione Europea, sulla base di quanto stabilito dalla Risoluzione del 2017, hanno sviluppato una serie di documenti e iniziative. Questi includono la Comunicazione sull'Intelligenza Artificiale per l'Europa,[214] il Piano Coordinato sull'Intelligenza Artificiale,[215] la Risoluzione sulla Politica Industriale Europea Globale per la Robotica e l'Intelligenza Artificiale,[216] la Comunicazione per Creare Fiducia nell'Intelligenza Artificiale Antropocentrica[217] e infine, il Libro Bianco sull'Intelligenza Artificiale.[218] Quest'ultimo

[213] Teubner G.; "*Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi*", ESI, 2019, p. 27 ss.
[214] Cfr. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, "*L'intelligenza artificiale per l'Europa*", del 25 aprile 2018
[215] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, "*Piano coordinato sull'Intelligenza Artificiale*", del 7 dicembre 2018
[216] Risoluzione del Parlamento europeo del 12 febbraio 2019 su una politica industriale europea globale in materia di robotica e intelligenza artificiale
[217] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, "*Creare fiducia nell'Intelligenza Artificiale antropocentrica*", dell'8 aprile 2019
[218] Commissione europea. "*Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*", 2020

documento affronta anche la questione della responsabilità civile nel contesto della sicurezza e dell'efficace funzionamento del regime di responsabilità. Si sottolinea l'importanza di avere disposizioni chiare sulla sicurezza che possano gestire i rischi associati alle transizioni tecnologiche, al fine di evitare pericoli per le persone coinvolte e incertezza legale per le imprese che vendono prodotti nell'Unione Europea contenenti sistemi di Intelligenza Artificiale. In particolare, si evidenzia la sfida nel determinare chi sia responsabile delle decisioni prese dai sistemi di IA, data l'opacità spesso associata a tali sistemi (il cosiddetto effetto "scatola nera"). Tuttavia, la Commissione sostiene che le attuali normative dell'UE sulla sicurezza dei prodotti e la responsabilità per danni causati da prodotti difettosi, comprese le norme settoriali e le leggi nazionali integrate, possano essere potenzialmente applicate anche ai sistemi di IA. Questa posizione è condivisa anche dal Parlamento europeo. La Commissione afferma che le persone che subiscono danni causati da sistemi di Intelligenza Artificiale dovrebbero beneficiare dello stesso livello di protezione di coloro che subiscono danni da altre tecnologie, ma senza compromettere la ricerca e lo sviluppo tecnologico.[219] Pertanto, è necessario esaminare attentamente tutte le opzioni disponibili per raggiungere questo obiettivo, compresa la possibilità di apportare modifiche alla Direttiva sulla responsabilità per danno causato da prodotti difettosi o di intraprendere ulteriori misure specifiche per armonizzare le normative nazionali in materia di responsabilità. Dopo la pubblicazione del libro bianco, si è intensificato lo scambio interdisciplinare, coinvolgendo non solo giuristi ed eticisti con diverse specializzazioni che normalmente non collaborano, ma anche studiosi di altre scienze, sia umane che esatte. Questo sforzo mira a superare le barriere disciplinari esistenti al fine di sviluppare una sorta di "*lex robotica*" destinata a regolare le interazioni tra esseri umani e macchine, nonché tra macchine stesse, nel rispetto dei diritti umani.[220]

[219] Cfr. Libro bianco sull'intelligenza artificiale
[220] Leanza C.; "*Intelligenza artificiale e diritto: ipotesi di responsabilità civile nel terzo millennio*", in Responsabilita' Civile e Previdenza, fasc.3, 1 marzo2021, pag. 1011

Da tenere certamente in considerazione in tale ambito è poi la proposta di regolamento, contenuta nella risoluzione del Parlamento UE, recante *"raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale"* del 2020, la si pone come obiettivo la definizione di un quadro giuridico certo in materia di responsabilità civile. Tale quadro rientra nella politica comunitaria volta alla costruzione di un'Intelligenza Artificiale che sia sicura ed affidabile e punta a instaurare un clima di fiducia verso la stessa. Quello della fiducia, secondo quanto previsto dalla proposta, è infatti un elemento fondamentale in quanto "*qualsiasi quadro giuridico in materia di responsabilità civile orientato al futuro deve infondere fiducia nella sicurezza, nell'affidabilità e nella coerenza di prodotti e servizi, compresa la tecnologia digitale, al fine di trovare un equilibrio tra l'efficace ed equa tutela delle potenziali vittime di danni o pregiudizi e, allo stesso tempo, la disponibilità di una sufficiente libertà d'azione per consentire alle imprese, in particolare alle piccole e medie imprese, di sviluppare nuove tecnologie e nuovi prodotti o servizi*"[221]

Nella proposta vi è poi un importante rinvio alla Direttiva sulla responsabilità per danno da prodotti difettosi; il Parlamento europeo ha evidenziato che, in linea di principio, la direttiva sulla responsabilità per danni da prodotti difettosi può rimanere fondamentale per affrontare la maggior parte dei danni causati dall'IA. Tuttavia, riconosce la necessità di apportare alcune modifiche per adattarla all'era digitale.[222] Questi cambiamenti mirano principalmente a ridefinire i concetti legali di "*prodotto*", per includere software, servizi digitali e la connessione tra diversi prodotti, e di "*produttore*", per coprire fornitori di servizi e fornitori di dati, in modo da garantire un adeguato risarcimento dei danni derivanti da queste tecnologie. Tuttavia, si

[221] Cfr. Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale, 2020/2014
[222] Cfr. Risoluzione del Parlamento europeo del 3 maggio 2022 sull'intelligenza artificiale in un'era digitale, 2020/2266

sottolinea anche l'importanza di evitare modifiche eccessivamente ampie o troppo restrittive in questo processo di aggiornamento normativo.

Altro pilastro da tenere in considerazione in tema di responsabilità è certamente l'AI Act; Tale proposta non regolamenta aspetti inerenti alla responsabilità civile dell'IA, ma si pone obiettivi specifici, come precedentemente proposto dalla risoluzione del Parlamento europeo sugli aspetti etici per l'IA, la robotica e le tecnologie correlate. Le questioni chiave prese in considerazione sono la definizione stessa di Intelligenza Artificiale, la suddivisione dei sistemi di IA in diverse categorie e l'identificazione di quali pratiche di IA dovrebbero essere vietate.

Quindi, al fine di fornire una visione di quella che potrebbe essere la regolamentazione della responsabilità civile dell'IA, vengono presi in considerazione tre strumenti. Il primo è l'Artificial Intelligence Act; il secondo strumento invece è la Risoluzione del Parlamento europeo concernente la responsabilità civile dell'IA del 2020; il terzo è invece rappresentato dalla direttiva sui danni da prodotto.[223]

[223] Chiappini D.; "*Intelligenza Artificiale e responsabilità civile: nuovi orizzonti di regolamentazione alla luce dell'Artificial Intelligence Act dell'Unione europea*" in Rivista italiana di informatica e diritto, fascicolo 2-2022

CONCLUSIONI:

La sfida che il diritto deve affrontare di fronte alle nuove e inedite realtà che emergono con lo sviluppo delle tecniche e dei sistemi di Intelligenza Artificiale è di natura veramente trasformativa. Questo contesto solleva interrogativi fondamentali sul futuro dell'umanità e sul genere di mondo che desideriamo costruire e in cui vogliamo vivere. Dobbiamo essere consapevoli del fatto che la questione ha una dimensione che va oltre il tempo presente, sia nel senso che l'Intelligenza Artificiale non rappresenta una fase temporanea nell'evoluzione tecnologica, ma piuttosto un cambiamento irreversibile nelle forme della nostra esistenza; sia nel senso che le decisioni che prendiamo o permettiamo oggi avranno conseguenze sulle generazioni future, sia adesso che in futuro.[224]

Ecco che proprio per questi motivi è necessario creare un diritto che non abbia paura del futuro, ma un diritto che senta il dovere di pensare al futuro, un diritto che renda possibile il futuro, un diritto che responsabilmente e ragionevolmente si preoccupa e si fa carico delle conseguenze nel tempo delle decisioni di oggi e dei problemi che è chiamato a regolare. La tematica dell'AI è sicuramente una tematica globale, ha certamente una dimensione tale che non può essere confinata geograficamente e forse anche dal punto di vista del diritto è a questo che dobbiamo mirare; la stessa UE nel corso del tempo con i propri lavori ha sottolineato come sia necessario uniformare la disciplina in tale ambito al fine di favorire uno sviluppo armonizzato e sicuro. Ecco che allora in un mondo sempre più interconnesso non si affacci in futuro la necessità di una disciplina, non solo sovranazionale come quella dell'UE, ma addirittura globale, con regole e principi condivisi in tutto il mondo. [225]

[224] D'Aloia A.; "*Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*" in BioLaw Journal – Rivista di BioDiritto, n. 1/2019, p. 56
[225] D'Aloia A; "*Generazioni future (diritto costituzionale)*", Milano, 2016 p. 356ss

L’Unione Europea com’è emerso da questo lavoro, cerca di porsi a capo di questa rivoluzione, non solo tecnologica ma anche legislativa a questo punto, tracciando la strada verso il futuro. Tuttavia, il percorso è ancora lungo.

Il GDPR e l’AI Act rappresentano sicuramente un passo in avanti nel voler regolare tale settore, ma allo stato attuale questi due atti sollevano dubbi, perplessità e problemi anche di coordinamento tra le relative discipline. Così l’AI Act, ad esempio, per com’è impostato sembra prevedere un ruolo sproporzionato per i fornitori e gli utenti di intelligenza artificiale nell’attuazione ed esecuzione del regolamento a causa dei dubbi, ad esempio, sugli strumenti di valutazione della conformità predisposti dal regolamento stesso. La stessa definizione di “*intelligenza artificiale*” sembra eccessivamente generica, specie in relazione ai sistemi di IA ad alto rischio. I requisiti obbligatori previsti per questi sistemi nel Titolo III Cap. 2 si basano sull'osservazione che un certo numero di diritti fondamentali è compromesso, in particolare, dalle caratteristiche speciali del machine learning, come l'opacità, la complessità, il comportamento autonomo. Poiché queste caratteristiche sono o assenti o presenti solo in parte negli algoritmi semplici la definizione ampia di intelligenza artificiale potrebbe portare a una sovra-regolamentazione. Allo stesso modo il rapporto tra l’AI Act e il GDPR sembra non essere sempre così complementare; questo, secondo il mio parere, per vari motivi. Il GDPR è stato progettato per essere una legge generale sulla protezione dei dati personali, mentre l'AI Act è più specifico per la regolamentazione dell'intelligenza artificiale. Ciò significa che il GDPR potrebbe non affrontare completamente le questioni legate all'IA, come l'opacità degli algoritmi o le decisioni automatizzate. Il GDPR offre principi generali sulla protezione dei dati, ma manca di orientamenti specifici sull'uso dell'IA. L'AI Act, d'altra parte, fornisce regole e requisiti dettagliati per i sistemi di intelligenza artificiale pur con le lacune e i dubbi già sottolineati. Lo stesso approccio dei due regolamenti è diverso; Il GDPR è spesso visto come un regolamento reattivo, poiché si concentra sulla protezione dei dati personali dopo che sono

stati raccolti. L'AI Act cerca di adottare un approccio più proattivo, stabilendo regole prima che i sistemi di intelligenza artificiale siano utilizzati in modo da prevenire potenziali danni. Ecco che dunque l'AI Act aggiungendo un ulteriore strato di regolamentazione alla panoramica normativa europea causa qualche problema di coordinamento e coerenza con il GDPR, specie in particolari zone grigie come, ad esempio, quando si tratta di sistemi di IA che trattano dati personali sensibili dove non sempre è chiara quale delle discipline deve prevalere

Se l'Unione europea desidera consolidare la sua leadership globale, deve assolutamente affrontare questi problemi di coordinamento tra queste due discipline che sono poste alla base del quadro giuridico europeo in materia di IA. Questo è l'obbiettivo primario che l'UE deve raggiungere per creare sistema uniforme e coerente che crei certezza e sicurezza all'interno di un settore che cambierà il mondo senza eguagli.[226]

L'evoluzione tecnologica è rapida ed impatta sempre di più sulle nostre vite; crea nuove opportunità e solleva questioni sociali e morali che pongono dilemmi all'uomo. Il diritto deve trovare il giusto equilibrio tra progresso e tutela degli individui, è un compito arduo ma è necessario assumere decisioni ponderate perché le scelte di oggi costruiscono il domani.

[226] Finocchiaro G.; "*La regolazione dell'intelligenza artificiale*" in Rivista Trimestrale di diritto pubblico, fasc. 4. 2022, p. 1098ss

BIBLIOGRAFIA

A. Raz., Minari J.;"*Ai-driven risk scores: shoul social scoring and polygenic scores based on etnicity be equally prohibited*" Edited by Manuel Corpas, University of Westminster, United Kingdom 30 maggio 2023, p. 20ss

Agata C.; "*Intelligenza artificiale, big data e nuovi diritti*", fascicolo 1-2022 Rivista Italiana di informatica e diritto, p. 94-97

Ali Alessio Salman "*Reti neurali artificiali: dal MLP alle più recenti architetture di Convolutional Neural Networks*" 2017

Alù A.; "*Esiste il diritto all'oblio su internet? La complessa evoluzione di tale figura tra giurisprudenza e legge*", in Diritto di famiglia e delle persone, n.1, 2020, 2, p. 313-328

Amidei A.; "*Robotica intelligente e responsabilità: profili e prospettive evolutive del quadro normativo europeo*", in Ugo Ruffolo, "*Intelligenza artificiale e responsabilità*", Giuffrè, 2017, p. 63-70

Barocas, A., Selbst D.; "*Big data's disparate impact*", Calif. L. Rev., 2021, p. 683

Baroglio C.; "*L'Intelligenza Artificiale? È un gioco!*" atti del convegno dimatica 7-8 ottobre 2021, Palermo

Bellomia V.; "*Diritto all'oblio e la società dell'informazione*", p. 244ss

Bobbio N.; "*L'età dei diritti*", Torino, 1990, p. 13-14

Borghi M.; ”*Portabilità dei dati e regolazione dei mercati digitali*” in Mercato concorrenza regole / a. XX, n. 2, agosto 2018, p. 228ss

Buyers J.; ”*Artificial Intelligence. The pratical legal issues*”, Londra, 2018, p. 43

Burr, C., Cristianini, N., Ladyman, J.; ”*An Analysis of the Interaction Between Intelligent Software Agents and Human Users*“, Minds and Machines, 28, 2018, p. 735-774

Bygrave L.A.; ”*Data Protection Law: Approaching Its Rationale, Logic and Limits*”, The Hague, 2002, p. 85ss.

Casonato C., Marchetti B.; ”*Prime osservazioni sulla proposta di regolamento dell’Unione Europea in materia di intelligenza artificiale*" in BioLaw Journal – Rivista di BioDiritto, n. 3/2021 p. 223-227

Chiappini D.; "*Intelligenza Artificiale e responsabilità civile: nuovi orizzonti di regolamentazione alla luce dell’Artificial Intelligence Act dell’Unione europea*" Fascicolo 2-2022, p. 90ss

Citino Y. M.; ”*Social scoring e città distopica: la profilazione del cittadino con finalità di policy urbana alla prova dei valori costituzionali*" in ”La città come istituzione, entro e oltre lo Stato” a cura di Allegri G., Frosina L., Guerra A., Longo A.; p. 117ss

Contissa G., Galli F., Godano F., Sartor G.; Rivista semestrale on-line: www.i-lex.it Dicembre 2021 Fascicolo 2

Cybersecurity Law of the People's Republic of China, 6 novembre 2016

D'Aloia A.; "*Il diritto verso "il mondo nuovo*". Le sfide dell'Intelligenza Artificiale" in BioLaw Journal –Rivista di BioDiritto, n. 1/2019, p. 56

D'Aloia A; "*Generazioni future (diritto costituzionale)*", Milano, 2016 p. 356ss

D'Anna A.; "*L'ambito di applicazione territoriale del regolamento generale per la protezione dei dati personali"*, a cura di Bonavita S.; "*Società delle tecnologie esponenziali e general data protection regulation: la circolazione internazionale dei dati personali*", Horisma, 2019, p. 61-83

D'Avanzo W.; "*Lotta alla pandemia e tutela della privacy*" Tigor: rivista di scienze della comunicazione e di argomentazione giuridica - A. XIV (2022) n.2

Data Security Law of the People's Republic of China, 10 giugno 2021

De Gregorio.; "*Privacy, tutela dei dati personali e Big Data*", Milano, 2022, p. 27-29

De Matos Pinto I.; "*The draft AI Act: a success story of strengthening Parliament's right of legislative initiative?*" ERA Forum, 2021

Decreto Legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, (c.d. "Codice della privacy")

Denley, A., Foulsham M., Hitchen B.; "*GDPR: how to achieve and maintain compliance*", 2019, p. 74-75

Di Ciollo G.; "*L'ambito di applicazione della normativa privacy: analisi comparata tra GDPR e direttiva 95/46/CE*", Iusinitinere, 2019,

Di Ciommo F.; "*Il diritto all'oblio nel Regolamento (UE) 2016/679 sul trattamento dei dati personali*", in Foro Italiano, fasc. 6, settembre 2017

Di Viggiano P.; "*Etica, Robotica e Lavoro: Profili D'Informatica Giuridica*",vol. 16, no. 22, 2018, p. 247-266

Dichiarazione Universale dei Diritti Umani, Assemblea Generale Nazioni Unite, approvata il 10 dicembre 1948

Dictionary.cambridge.org/it/, s.v., "*artificial intelligence*", disponibile presso ARTIFICIAL INTELLIGENCE | definizione, significato - che cosa è ARTIFICIAL INTELLIGENCE nel dizionario Inglese - Cambridge Dictionary

Dignum V.; "*Responsible artificial intelligence: how to develop and use AI in a responsible way*", Springer Nature, 2019, p. 120

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 del Parlamento europeo e del Consiglio, del 24 ottobre 1995

Enciclopedia Treccani definizione "intelligenza artificiale"; intelligènza artificiale nell'Enciclopedia Treccani

Faro S.; Informatica e diritto, XXX annata, Vol. XIII, 2004, n. 1-2, p.14-15

Ferrari V.; Note socio-giuridiche introduttive per una discussione su diritto, intelligenza artificiale e big data 24 Novembre 2020

Ferretti F.; ”*Data protection and the legitimate interest of data controllers: much Ado about nothing or the winter of rights*?“, in Common Market Law Review, 2014 p. 512

Fidanza F.; ”*Sul concetto di intelligenza artificiale*”, La Nuova Giuridica, 1/2022

Finocchiaro G.; “*La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*” pubblicato su “Il diritto dell’informazione e dell’informatica” Anno XXX Fasc. 4-5 -2015

Finocchiaro G.; Diritto dell'Informazione e dell'Informatica (Il), fasc.2, 1 aprile 2022, p. 303

Finocchiaro G.; Rivista Trimestrale di Diritto Pubblico, fasc.4, 1 dicembre 2022, p. 1085

Finocchiaro G.; "*La regolazione dell'intelligenza artificiale*" in Rivista Trimestrale di diritto pubblico, fasc. 4. 2022, p. 1098ss

Floridi L.; "*The European Legislation on AI: a Brief Analysis of its Philosophical Approach*", 34 Philosophy and Technology 215, 2021

Green M., Nørgaard L., Cyril B., Birkedal B.; ”E*arly Modern Privacy: Sources and Approaches”,* MetteIntersections, 2022, p. 78-80

Guidotti R.; “*A survey of methods for explaining black box models*“, ACM computing surveys (CSUR), 2022, p. 15ss

Isaelli M.; "S*annzioni e responsabilità in ambito GDPR*", Compliance, 2019

Jann Stinnesbeck, Research Division Legislative Counsel Bureau, “R*esearch Brief On 65Autonomous Vehicles*” (Novembre 2017), disponibile online presso

https://www.leg.state.nv.us/Division/Research/Publications/ResearchBriefs/AutonomousVehicles.pdf

Krzysztofek M.; ”*GDPR: Post-Reform Personal Data Protection in the European Union*”, 2018, p. 18

Lavorgna, A., Suffia, G.; ”*La nuova proposta europea per regolamentare i Sistemi di Intelligenza Artificiale e la sua rilevanza nell'ambito della giustizia penale: un passo necessario, ma non sufficiente, nella giusta direzione*“, Diritto Penale Contemporaneo, 2021, p. 88-103

Leanza C.; ”*Intelligenza artificiale e diritto: ipotesi di responsabilità civile nel terzo millennio*”, in Responsabilita' Civile e Previdenza, fasc.3, 1 marzo2021, p. 1011

Libro Bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia - Bruxelles, 19.2.2020 COM(2020) 65 final

Longo G.; "*Big Data e intelligenza artificiale: che futuro ci aspetta*?" n. 20.2018, p. 101ss

Maglio, M.; “*Manuale di diritto alla protezione dei dati personali – La privacy dopo il regolamento UE*”. Milano, Maggioli Editore, 2017, p. 43

Mangiameli A.; "*Intelligenza artificiale, big data e nuovi diritti*"; Fascicolo 1-2022 Rivista Italiana di informatica e diritto, p. 75ss

Marini, P.; “*GDPR: il nuovo regolamento europeo sulla privacy*”. Milano: Edizione Ipsoa. 2017, p. 52

Marseglia G.; ”*AI Act: Impatti e Proposte. Opportunità e rischi dell'over-e under-regulation*" Article on ResearchGate, 2022, p. 21ss

McCathy J.; “W*hat is Artificial Intelligence*”, 2007, reperibile in: http://www- HYPERLINK "http://www-formal.stanford.edu/jmc/whatisai.pdf"

McDonald A.M.; ”*The Cost of Reading Privacy Policies*“ in I/S: A Journal of Law and Policy for the Information Society, p. 4ss

Messina A.; (2017) “*Privacy e regolamento europeo*”. Milano, Edizione Ipsoa, 2019

Mitchell T. M.; ”*Machine Learning*”, McGraw-Hill 1997

Mokander J.; ”C*onformity assessments and post-market monitoring: a guide to the role of auditing in the proposed European AI Regulation*“, Minds and Machines, 2021, p. 1-28

Moretti S.; ”*La Convenzione Europea dei Diritti dell’Uomo compie 70 anni*” Questione di Giustizia, 2020

Moro P., "*Intelligenza artificiale e tecnodiritto. Fondamenti etici ed innovazione legislativa*", in Moro P. (a cura di), "Etica, Diritto e Tecnologia. Percorsi dell'informatica giuridica contemporanea", Franco angeli, Milano 2021 p. 7-24 (p.17-18)

Napolitano C., ”*Il diritto all’oblio: la centralita’ dell’identita’ personale*“, in Danno e Resp., n. 6, 2020, p. 732ss

Orlando S.; ”*Regole di immissione sul mercato e pratiche di intelligenza artificiale vietate nella Proposta di Artificial Intelligence Act*” in ”Persona e Mercato” 2022/3 p. 346ss

Palmieri A.; ”*Dal diritto all’oblio all’occultamente in rete*“, in Foro it., 2014, p. 1-16

Panattoni B.; Diritto dell'Informazione e dell'Informatica (Il), fasc.2, 1 aprile 2021, p. 317

Partipilo F., "*La Dichiarazione Universale dei Diritti Umani dal 1948 ai nostri giorni*", Osservatoriodiritti, 2018

Pasquale F.; "*The Black Box Society. The Secret Algorithms That Control Money and Information*", 2015

Personal Information Protection Law of the People's Republic of China, 20 agosto 2021

Perugini R.; "*Il Data Protection Officer: le caratteristiche e i connessi profili di responsabilità*" European Journal of Privacy Law & Tchnologies, 2019, p. 25ss

Proietti G. "*Il libro bianco sull'intelligenza artificiale. L'approccio europeo tra diritto ed etica*" Giustiziacivile.com n. 6/2020

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

Raffiotta E., C., Baroni M.; "*Intelligenza artificiale, strumenti di identificazione e tutela dell'identità*" BioLaw, 12 aprile 2022, p. 165-172

Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati, Gazzetta ufficiale del 12/01/2001

Regolameto (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)

Riccio G. M.; ”*Gdpr e normativa privacy*” a cura di Giovanni Maria Riccio, Guido Scorza, Ernesto Blisario ”*Gdpr e normativa privacy*”, Milano, IPSOA, 2018, p. 4-9

Riccio. M.; ”*Data Protection Officer e altre figure*" in ”*La Nuova Disciplina Europea della Privacy*“, a cura di Sica S., D‘Antonio, Riccio M., Milano, 2016, p. 41ss

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

Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL))

Roberts H.; ”A*chieving a ‘Good AI Society': Comparing the Aims and Progress of the EU and US*”, 2019, p. 50

Sanguinetti G.; ”*Machine Learning: accuratezza, interpretabilità e incertezza*” Ithaca: Viaggio nella Scienza XVI, 2020 • Machine Learning Uncertainty, p. 78

Schneider G.; Responsabilità Civile e Previdenza, fasc.3, 1 Marzo 2023, p. 1014

Searle John R.; ”*Minds, Brains and Programs, in The Behavioral and Brain Sciences*”, 1980, Cambridge University Press

Soffientini M., Caccialupi M.; ”*Privacy: protezione e trattamento dei dati*”, PSOA Manuali, 2018, p. 53-55

Somalvico M.; 1987 “*L’Intelligenza artificiale*”, Rusconi, Milano

Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU, Settembre 2012.

Stoddart J., Chan B., Joly Y., ”*The European Union’s Adequacy Approach to Privacy and International Data Sharing*“ edited by Rothstein M., A; Knoppers B.M., The Journal of law, medicine & ethics, 03/2016, Volume 44, Fascicolo 1

Terolli E.; Diritto dell'Informazione e dell'Informatica (Il), fasc.1, 2021

Teubner G.; ”*Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi*“, ESI, 2019, p. 27 ss

Tosi E., Soro A., Franceschelli V., ”*Privacy digitale: riservatezza e protezione dei dati personali tra GDPR e nuovo Codice privacy*”, DNT Milano, Italy, 2019, p. 15ss

Turilli M.; ”*The ethics of information transparency, in Ethics and Information Technology*”, 2009, p. 11ss

U.S. Congress, Senate, “Future of Artificial Intelligence Act of 2017”, S 2217, 115th Cong., 63 1st sess., introduced in Senate December 12, 2017, disponibile presso https://www.congress.gov/bill/115th-congress/senate-bill/2217/text

Vanegas J. G.; ”*La violazione dei requisiti di sicurezza informatica di cui all'art 32 del GDPR", pubblicato su "Il diritto dell'informazione e dell'informatica*” Fascicolo 2-2020

Viterbo A.; Dir. informatica, fasc.4-5, 2007, p. 725

Warren S. D., Brandies L. D.; ”Right to privacy”, in Harvard Law Review, 1980 p. 194-195

Zorzi Galgano N.;. ”*Persona e Mercato Dei Dati. Riflessioni Sul GDPR",* CEDAM, 2019, p. 35-42