

UNIVERSITÀ DELLA VALLE D'AOSTA  
UNIVERSITÉ DE LA VALLÉE D'AOSTE

DIPARTIMENTO DI SCIENZE ECONOMICHE E POLITICHE  
CORSO DI LAUREA IN SCIENZE POLITICHE E RELAZIONI INTERNAZIONALI

ANNO ACCADEMICO 2021/2022

TESI DI LAUREA:  
ANALISI DELLE PROBLEMATICHE LEGATE ALL'IMPIEGO DELL'INTELLIGENZA  
ARTIFICIALE, IN RIFERIMENTO AL CONTESTO NORMATIVO E POLITICO  
DELL'UNIONE EUROPEA.

DOCENTE relatore: Prof. Bryan Weston Wylly

STUDENTE: 18 F02 424 ALBERTO COSENTINO

## INDICE:

- Introduzione	
- Capitolo Primo	1
<b>Nascita, diffusione e possibile sviluppo dell'Intelligenza Artificiale.</b>	
- 1.1 – Breve storia dell'Intelligenza Artificiale.	1
- 1.2 – Attuali impieghi dell'Intelligenza Artificiale.	4
- 1.3 – L'Intelligenza Artificiale nel contesto geopolitico attuale.	7
- 1.4 – L'Intelligenza Artificiale nella politica interna.	12
- 1.5 - “The age of surveillance capitalism”.	15
- 1.6 – Intelligenza Artificiale e ambiente.	22
- Capitolo Secondo	28
<b>Analisi delle problematiche legate all'uso dell'Intelligenza Artificiale.</b>	
- 2.1 – Il modello LIME	30
-Capitolo Terzo	33
<b>La normativa vigente nell’Unione Europa e le politiche attuali in materia.</b>	
- 3.1 – Le normative successive al GDPR	37
- 3.2 – European Data Strategy	42
- Conclusioni	47
- Bibliografia	52

## Introduzione

Il seguente testo intende, in riferimento al contesto socio-economico attuale, analizzare alcune delle problematiche derivate dall'impiego dell' Intelligenza Artificiale (IA).

A questo proposito è riportata brevemente la storia di questa tecnologia, che testimonia la velocità con la quale la stessa si sviluppa, e che la rende perciò temibile per molti aspetti. Vi sono poi descritte le principali applicazioni attuali, soffermandosi in particolare sulle implicazioni politiche e sul paradigma economico derivante da queste, a dimostrazione del suo già massiccio impiego. Oltre a ciò sono riportate le attuali normative in materia, nel contesto dell'Unione Europea.

Il testo analizza inoltre un caso “emblematico”, che dimostra l'incombenza dei problemi legati alle decisioni, sempre più importanti e vincolanti, che tali algoritmi prendono quotidianamente. Tale caso evidenzia la necessità di rispondere tempestivamente attraverso adeguate soluzioni normative e altri strumenti di tutela degli utenti.

In aggiunta l'argomento viene trattato dal punto di vista ambientale, si ritiene importante includere tale aspetto in quanto l'IA risulta particolarmente legata al cambiamento climatico in corso.

Da un lato infatti essa contribuisce e ragionevolmente contribuirà in maniera sempre più pesante alle emissioni inquinanti in futuro, ma d'altro canto potrebbe rivelarsi uno strumento fondamentale nel garantire il futuro del pianeta. La discussione riguardo all'uso di tale tecnologia non può quindi non includere tale aspetto.

Sebbene non esista al momento una definizione universalmente accettata di Intelligenza Artificiale, una delle più autorevoli proviene da un documento patrocinato dalla Commissione europea e redatto da un gruppo di esperti nel settore:

*“Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals.*

*AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or*

*AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications).* [1]

Per IA, si intende quindi una serie di tecniche e sub discipline con approcci e caratteristiche diverse come l'apprendimento automatico e la robotica.

A partire da qualche decennio l'Intelligenza Artificiale sta invadendo sempre più settori. Originariamente legata al desiderio umano di ricreare la nostra intelligenza, essa, in maniera crescente e sempre più profonda, gestisce e regola svariati aspetti della nostra vita: ad esempio selezionando le notizie che vediamo sui Social Network, determinando in alcuni casi l'orario di lavoro o il salario, occupandosi della sicurezza anti terrorismo. Visto il crescente sviluppo e impiego di tali tecnologie è logico ipotizzare che l'IA negli anni a venire sarà responsabile di decisioni ancor più rilevanti, pensiamo ad esempio alle auto intelligenti o ai robot chirurgici. Oltre a ciò siamo testimoni del lento ma continuo progresso che avvicina le macchine ad un perfetta imitazione della nostra intelligenza.

La tecnologia da decine di migliaia di anni ha progressivamente sostituito l'uomo nelle mansioni fisiche o manuali, mettendosi in competizione e superando la forza o la capacità umana di svolgere determinati compiti. Essa ha consentito all'essere umano di aumentare esponenzialmente la sua capacità di agire.

La nostra specie, si distingue nel regno animale per la capacità di rispondere a problemi complessi. Secondo la legge dell'evoluzione, in un ambiente selvaggio, come quello in cui l'uomo si è evoluto, gli esseri viventi, per garantire la propria sopravvivenza, [2] compensano la propria inferiorità fisica affinando particolari abilità. L'uomo è riuscito a fare ciò grazie alla tecnologia. Altre specie, ad esempio, compensano la propria vulnerabilità specializzandosi in determinate strategie di sopravvivenza, pensiamo ad esempio ai camaleonti. [3]

In particolare l'uomo è stato in grado, tramite l'utilizzo di strumenti, di compensare la propria inferiorità fisica, come l'assenza di "armi naturali", ad esempio zanne e artigli. Esse consentivano ad esempio ai grandi carnivori preistorici di procacciarsi un fabbisogno calorico inaccessibile agli ominidi. Oltre a ciò, quest'ultimi erano sprovvisti di un apparato digerente in

grado di ingerire carne cruda, e di conseguenza di beneficiare del circolo virtuoso derivante da una dieta più ricca [4].

Invenzioni come le lance rudimentali hanno permesso agli ominidi di procacciare prede assai più grandi, con un valore nutritivo decisamente più elevato, prima accessibili ai soli carnivori. [5]

La scoperta del fuoco ad esempio ha consentito la possibilità di assimilare molte più calorie, garantendo quindi chances notevolmente maggiori di sopravvivenza.

Oltre a ciò la cottura delle prede e la loro assimilazione è stata resa possibile sempre dal fuoco, in quanto i nostri antenati non erano dotati di zanne adatte ad ingerire carne cruda.[6] Via via sono seguite ulteriori scoperte, come ad esempio l'agricoltura. La tecnologia dunque ha permesso all'uomo di sopravvivere in un ambiente ostile, di scalare la piramide alimentare e di diventare la specie dominante.

Nonostante l'essere umano non sia l'unica specie in grado di utilizzare degli utensili, l'uso degli strumenti da parte dell'uomo, ha permesso ad esso di aumentare esponenzialmente la propria capacità di agire. Tanto da poter alterare, accelerandolo esponenzialmente, il naturale processo evolutivo.

L'uomo col tempo ha acquistato una capacità di agire sull'ambiente tale da accelerare le leggi evolutive precedenti, modificando il paesaggio, stravolgendo gli equilibri biologici, facendo estinguere o proliferare altre specie animali e il clima.

La possibilità di controllare l'ambiente circostante in maniera da soddisfare i propri bisogni, ha alterato il naturale adattamento della specie umana al proprio habitat.

Sin dalla scoperta dei primi utensili la tecnologia continua ad evolversi, l'uomo oggi inizia con l'IA ad esplorare la possibilità di creare una forma di intelligenza che superi gli stessi limiti umani.

Le ipotesi sul futuro dell'IA dividono esperti ed accademici in opinioni contrastanti: alcuni come il filosofo Nick Bostrom (2003) o Kurzweil (The singularity is near, 2005)[7] dichiarano inevitabile il sorpasso dell'intelligenza artificiale su quella umana, Bostrom teme l'eventualità che l'IA possa determinare la nostra estinzione, [8] sostenendo che in un futuro più o meno prossimo l'IA sorpasserà l'uomo, e diventerà l'entità dominante, minacciando quindi la nostra esistenza.

Sempre Bostrom e Kurzweil descrivono questo cambiamento come imminente, data infatti la velocità esponenziale con il quale aumenta la potenza di calcolo dei processori (legge di Moore), [9] ed in generale con il quale si evolve la tecnologia informatica [10]; essi sostengono inoltre che tale rivoluzione avverrà nei prossimi cent'anni, portando invenzioni fantascientifiche come l'implementazione di parti meccaniche nel corpo umano o addirittura la creazione di veri e propri cyborg (un ibrido tra uomo e macchina) [11].

Queste tesi evidenziano i limiti fisici del cervello umano: ovvero il fatto che esso è limitato dalle dimensioni della scatola cranica, di contro un computer può raggiungere le dimensioni di un magazzino.

Inoltre la velocità con cui si muovono le informazioni nel nostro cervello è decine di volte inferiore alla velocità dei moderni processori [12].

Altri esperti come l'inventore dei rivoluzionari microprocessori, F. Faggin, sono più scettici a riguardo, egli considera i cambiamenti annunciati da Bostrom come assai lontani dal presente, visti i grandi limiti dell'IA attuale.[13]

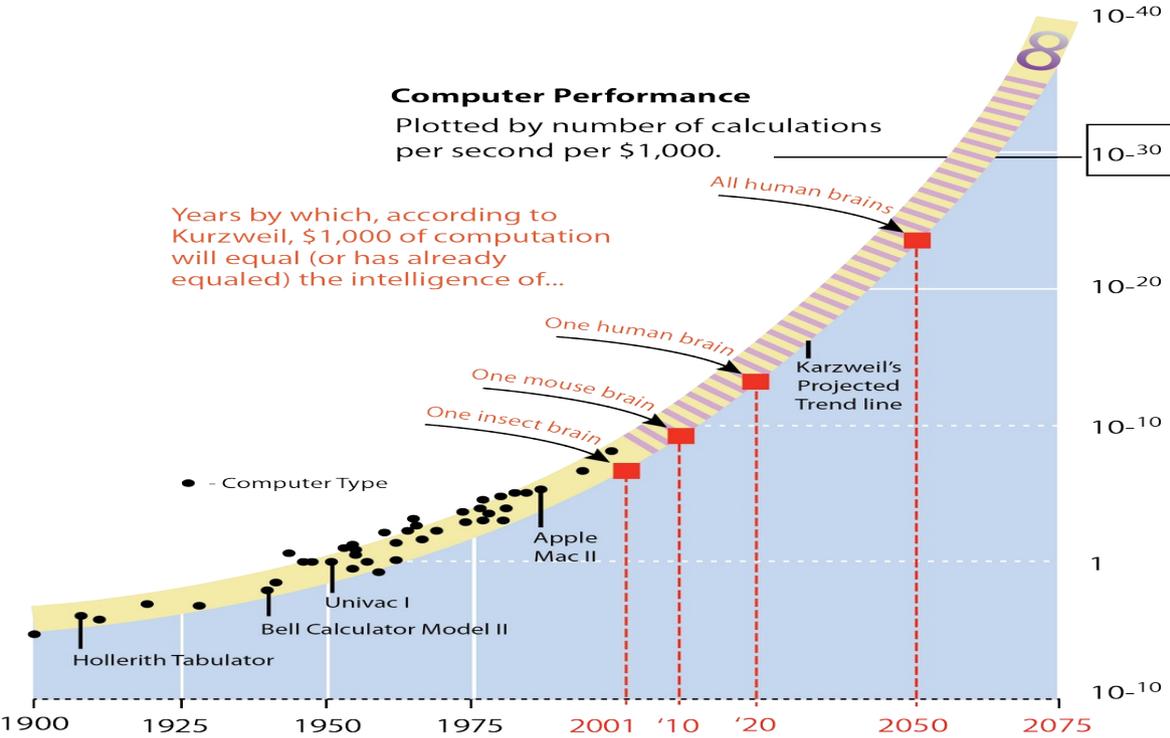
In primo luogo a causa della “ristrettezza” delle capacità delle varie tecnologie attualmente impiegate. Ad oggi esse infatti riescono ad eseguire determinati compiti tipici dell'uomo, in alcuni casi con performance sovraumane, ma sempre e comunque in un ambiente circoscritto o svolgendo un compito limitato.

Pensiamo ad esempio all' algoritmo di Google, Alpha Go, che nel 2016 è riuscito a sconfiggere il campione del mondo del gioco di strategia orientale, Go.

Il passaggio dalla attuale IA limitata ad un IA generale, in grado di imitare in toto una forma di vita come l'intelligenza naturale, non è quindi assolutamente scontato e richiede la risoluzione di problemi per ora insormontabili.

Riassumendo, la velocità con cui la tecnologia evolve è esponenziale: ad esempio l'umanità ha impiegato milioni di anni per sviluppare un linguaggio complesso. Decisamente inferiore è stato il tempo richiesto per l'invenzione della scrittura, in seguito è passato qualche millennio per elaborare i concetti matematici filosofici. Infine sono bastati un paio di secoli per tradurre tali concetti nel linguaggio logico adatto e per raggiungere le conoscenze chimico fisiche per la costruzione dei computer. In base a tale tendenza non è quindi da escludere che in futuro

remoto le ipotesi di Bostrom si avverino, ad oggi comunque il futuro delle macchine e forse della stessa umanità rimane incerto. [15]



Il grafico descrive lo sviluppo tecnologico nel tempo, mostrando come tale fenomeno sia esponenziale/iperbolico.

## Capitolo Primo

### **Nascita, diffusione e possibile sviluppo dell'Intelligenza Artificiale.**

#### - 1.1 Breve storia dell'Intelligenza Artificiale

Difficile stabilire una data precisa per la nascita dell'IA: già gli antichi greci avevano immaginato delle macchine nate per mano dell'uomo, in grado di muoversi e interagire. Troviamo degli esempi nei miti classici di Talo [1] o nelle statue di bronzo create da Dedalo. Anche altre culture antiche definiscono questo concetto di imitazione della natura, in un testo islamico di alchimia del IX sec. è presente questo concetto, così come per il “golem” del folklore ebraico.[2]

Sebbene il termine Intelligenza Artificiale risalga al secolo scorso, si intravede in questi esempi un certo legame con l'idea moderna di IA. Inoltre dai tempi di Omero sono stati fatti molteplici tentativi di creare un automa, ad esempio il cavaliere meccanico di Leonardo Da Vinci. Fino al secolo scorso non si possedeva però un linguaggio matematico adeguato, né materiali adatti a costruire tali macchine.

Questo linguaggio matematico deriva dalla logica classica, databile dai tempi di Aristotele, ovvero la disciplina che analizza il ragionamento con lo scopo di definire la correttezza dei procedimenti inferenziali del pensiero.

Bisogna quindi attendere millenni per lo sviluppo di un linguaggio matematico concretamente applicabile.

Nel XVII sec. Il filosofo e matematico G.Leibnitz, (1646-1716) elabora un sistema filosofico basato su una logica binaria. [3] Altri autori come T.Hobbes, (1588–1679) arrivano alla conclusione che il pensiero umano sia definibile in termini meccanicistici. [4]

Più tardi nel XIX sec. George Boole, (1815-1864) ispirato dal lavoro di Leibniz, elabora un sistema logico in grado di rappresentare tramite un'equazione una qualsiasi affermazione.

All'epoca la logica di Boole risultò però arida di applicazioni, solo nel 1886 dopo anni di studi del suo sistema, esso venne concretamente applicato[5].

Il primo tentativo di realizzare una macchina computazionale (ovvero un calcolatore analogico), avviene grazie agli sforzi di Charles Babbage, (1791-1871) [6] che negli anni 40' del XIX sec. progetta svariati modelli di tali macchine senza riuscire pienamente nell'intento. I vari progetti vengono inizialmente finanziati dalla corona britannica che poi abbandona lo scienziato. Senza dubbio all'epoca di Babbage mancava la tecnologia adatta a tale scopo.

Solo nel XX secolo i progressi nelle scienze sperimentali portano allo sviluppo delle discipline statistiche, consentendo l'elaborazione di equazioni inferenziali derivate dai dati. Nel 1936 il matematico inglese Alan Turing (1912-1954) è il primo a unificare gli sforzi precedenti elaborando il concetto astratto, alla base degli odierni computer, nel saggio “la macchina pensante”.

Nei testi seguenti, Turing immagina la possibilità di simulare attraverso i computer l'intelligenza umana, oltre a descrivere i metodi utilizzati ancora oggi con cui l'IA dev'essere testata e allenata. Turing riuscirà solo parzialmente nel creare le macchine immaginate, come Babbage egli rimane limitato dalla tecnologia dell'epoca. [7]

Successivamente negli Anni '50 l'Intelligenza Artificiale emerge come disciplina, il termine IA viene infatti utilizzato per la prima volta nel 1956 da J.Mccarthy (1927-2011). [8] Inoltre nel 1955 Simon (1916-2001) e Newell (1927-1992) nel tentativo di rappresentare il processo cognitivo umano elaborano i primi algoritmi, precursori dell'IA moderna; il Logic Theorist Program e in seguito il General Problem Solver.[9]

Quasi contemporaneamente a Turing, il tedesco Konrad Zuse (1910-1995) realizza il primo computer programmabile, oltre alla macchina di Zuse viene costruito Colossus nei laboratori britannici, mentre in America nasce il progetto ENIAC, diretto dal matematico di origini ungheresi Von Neumann (1903-1957).[10]

Proprio negli anni 50' e 60' lo sviluppo dei computer decolla grazie all'impulso dato dalla ricerca militare: nascono i 3 principali campi di ricerca dell'IA. Il primo modello di rete neurale ispirato al cervello umano viene creato nel 1949 per mano di McCulloch (1898-1969) e Pitts (1923-1969). Il machine learning compare nel 1959 ad opera di Samuels (1901-1990), i

chatbot nel '64, (il primo esemplare si chiama ELIZA e fu inventato dal tedesco J. Weizenbaum) (1923-2008). Degno di nota è poi “Shakey” (1966), un robottino dotato di ruote in grado di muoversi autonomamente, precursore della robotica moderna. [11] Maggiori risorse pubbliche e private vengono investite negli anni successivi per lo sviluppo dei primi Computer, grazie a questo impulso nascono in questi anni Wi-Fi, GPS e Internet, fondamentali per gli ulteriori sviluppi dell'IA. [12]

Nonostante gli iniziali e promettenti progressi, negli Anni 80' la ricerca non ottiene importanti applicazioni pratiche, rimanendo ancora evidente il gap tra teoria e pratica. In particolare nel superare la binarietà della logica booleana (Vero/Falso), rendendo quindi difficoltoso quantificare l'incertezza e l'aleatorietà del mondo reale. Nonostante ciò in questi anni cresce esponenzialmente la potenza dell'hardware. Diminuisce il costo dei processori, aumenta contemporaneamente la memoria di questi, di conseguenza cresce la capacità di analizzare grandi quantità di dati. Ciò permette quindi di affinare le funzioni statistiche su cui si basano gli algoritmi.

Lo sviluppo dell'IA ritrova vigore negli Anni '90, attirando l'attenzione dei media in seguito alla vittoria del Computer Deep Blue di IBM sul campione del mondo di scacchi Kasparov nel 1997[13]. Per la prima volta un Computer è in grado di misurarsi con l'intelligenza umana, dimostrando di riuscire a controllare un universo platonico e limitato qual'è una scacchiera.

Negli Anni 2000 nascono il metodo di apprendimento “Deep learning” [14], che permette alle reti neurali, eredi dell'invenzione di Mcculloch e Pitts, di apprendere in maniera automatica dai dati immessi, e quindi eseguire operazioni molto più complesse rispetto alle tecnologie precedenti.

A partire dagli Anni 2000, causa la diffusione di Internet prima e dei Social Network poi, sempre più utenti generano e condividono quotidianamente una mole smisurata di dati. Gli algoritmi, essendo basati su una funzione statistica, più sono alimentati dai dati più riescono ad affinare le loro capacità predittive, processo di cui si occupa una delle discipline più importanti dell'IA, la Big Data analysis. Tali tecnologie, combinate alle tecniche marketing, hanno dato vita ad un mercato assai redditizio (descritto nel capitolo 1.5), denominato da S.

Zuboff “Surveillance Capitalism”. Esso è stato negli anni monopolizzato da Google, Amazon e Facebook. Il loro successo nel settore le ha rese le compagnie più ricche e influenti al mondo.

## 1.2 – Attuali impieghi dell'Intelligenza Artificiale.

*“Oggi gli algoritmi sono ovunque”* Pedro Domingos, professore di Computer Science alla Washington University.

L'IA attuale, rispetto agli esseri senzienti dei film di fantascienza è in grado di occuparsi di singoli compiti, la sua capacità supera le performance umane già in molti settori e la sua presenza è massiccia già oggi.

Il termine intelligenza artificiale, evoca appunto l'immagine di un'entità senziente, in grado di eguagliare o persino superare in toto il cervello umano. Tra gli esempi più celebri, possiamo citare il computer HAL di Odissea nello Spazio di Stanley Kubrick, o l'androide immaginato nel romanzo di Isaac Asimov, Io Robot. Da tali esempi si può evincere la sostanziale differenza tra l'IA attualmente impiegata, la quale è in grado di svolgere mansioni ristrette o compiti limitati e l'IA immaginata in tali opere.

Esperti come Brossard classificano appunto le tecnologie attuali con il termine “narrow AI”, ad indicarne proprio i limiti attuali. Il secondo tipo, corrispondente agli esempi precedenti, viene invece definito: “GOFAI” (Good Old Fashioned Artificial Intelligence)[1], il termine fa riferimento al periodo d'oro dell'IA e della letteratura fantascientifica negli anni 50' del '900. All'epoca infatti, come riportato nel capitolo precedente, nacquero le principali discipline dell'IA, nel mezzo di tale fermento, gli studi di scienziati brillanti come Alan Turing facevano prospettare la rapida ascesa dei computer da semplici calcolatori ad esseri eguali a noi. La letteratura fantascientifica ha assimilato tale entusiasmo creando le immagini diffuse ancor'oggi.

La presenza dell'IA oggi raggiunge già diversi settori, tra cui: trasporti, internet, medicina, servizi finanziari, intrattenimento, informazione, difesa militare, sicurezza e marketing.

Dal punto di vista economico l'IA ha e in futuro avrà un effetto ancor più dirompente, in primo luogo sul mercato del lavoro e sulla produttività in generale.

Secondo un report del Parlamento Europeo l'impiego sempre più diffuso dell'IA, consentirebbe di raddoppiare il tasso di crescita dell'economia globale, entro il 2035 [2]. E' opportuno però considerare anche alcuni effetti secondari: in primis, la questione riguardante la distribuzione della ricchezza generata dall'automatizzazione del lavoro, la quale implica la soppressione di parecchie mansioni. Secondo un report del think-tank Bruegel, nei prossimi 20 anni il 54% dei posti di lavoro potrebbe essere computerizzato. [3]

Questo comporterebbe inoltre in una probabile polarizzazione: con una forte richiesta di mano d'opera non specializzata e con salari minimi, ed una parallela crescita di domanda per i lavori specializzati. Ciò implicherebbe un aumento della produzione, non rispecchiato però da un equivalente aumento dei consumi, con prevedibili effetti nefasti.[4]

Sotto diversi aspetti, si teme in aggiunta un'ulteriore concentrazione di potere nelle mani di poche grandi compagnie detentrici di tali risorse; il che potrebbe aggravare le diseguaglianze economiche, sia all'interno dei paesi sviluppati, ad esempio con la sopra citata polarizzazione del lavoro, sia tra paesi industrializzati e paesi in via di sviluppo.

L'impatto dell'IA sull'economia si può definire quindi incerto, in quanto potrebbe generare effetti opposti alle previsioni, oppure avere conseguenze prevalentemente negative in una prima fase, ad esempio molti posti di lavoro potrebbero essere soppressi in un breve periodo senza un ricambio immediato. Gli effetti virtuosi infatti potrebbero emergere solo in seguito, magari grazie ad una risposta normativa in grado di stabilizzare il mercato. [5]

In particolare una delle applicazioni più redditizie dell'IA consiste nella profilazione degli utenti di internet a fini di marketing. In tale mercato, la materia prima è la mole di dati che costantemente ogni utente genera nell'utilizzare dispositivi tecnologici. Come sostiene S.Zuboff, [6]quella che stiamo vivendo oggi è una vera e propria rivoluzione economica, altrettanto dirompente quanto la precedente rivoluzione industriale. Proprio come allora risulta complicato limitare gli eccessi di questa nuova economia, dalla mancanza di un'adeguata educazione verso le nuove tecnologie, oltre all'assenza di politiche adeguate a difesa della privacy degli utenti.

L'estrazione di queste informazioni rappresenta quindi una preziosa moneta di scambio in quanto è utilizzata per profilare, e in seguito influenzare gli utenti tramite l'esposizione di annunci personalizzati.[7]

Oltre alle applicazioni già citate, è opportuno menzionare altri settori che sono o saranno profondamente influenzati dall'IA: è prossima l'introduzione nel mercato delle auto intelligenti, che ha già alle spalle più di un decennio di intensa ricerca, secondo un'indagine del Parlamento Europeo è prevista la commercializzazione di auto completamente autonome a partire dal 2030. [8] Già ad oggi alcuni modelli in commercio hanno implementato alcune tecnologie per la guida assistita.

Robot domestici: gli aspirapolvere automatizzati sono presenti sul mercato già dai primi anni 2000, a partire dagli ultimi anni si sono diffusi gli assistenti digitali, nei prossimi 15 anni se ne prevede quindi una massiccia diffusione dovuta al significativo progresso dei sensori 3D. [9]

Grazie alle tecnologie di cloud computing, i vari dispositivi domestici, come già in realtà avviene, comunicano tra loro le informazioni raccolte. Vista la pervasività che caratterizza questi dispositivi, si tratta un settore particolarmente delicato per la tutela della privacy.

Nell'ambito sanitario l'impiego dell'IA risulta valido nelle analisi cliniche: particolarmente si prevede inoltre nel prossimo futuro la diffusione di infermieri e chirurghi robot.

Cura degli anziani: l'IA dovrebbe sostituire gli operatori sanitari nella cura degli anziani, presto potrebbero infatti essere operativi robot per il supporto sia emotivo che fisico del paziente.[10]

Sorveglianza e pubblica sicurezza: attualmente paesi come gli USA impiegano algoritmi a scopo di difesa anti-terrorismo o addirittura in campo giudiziario.

Nell'immediato futuro ci si aspetta che tale uso occupi maggiori funzioni, come la determinazione di misure preventive da parte di algoritmi. Il ruolo della tecnologia potrebbe

dunque in breve tempo spostarsi da semplice strumento a vero e proprio collaboratore delle forze dell'ordine e del sistema giudiziario. [11]

Nella sicurezza, come in molte altre applicazioni dell'IA, rimane ancora difficilmente conciliabile un bilanciamento chiaro tra l'invasività di tali dispositivi e il rispetto dei diritti personali. Oltre a ciò strumenti come i sistemi di sorveglianza sollevano questioni sulle probabili concentrazioni di potere che derivano dall'uso di tali tecnologie.

Come dimostra lo scandalo di Cambridge Analytica, (trattato in maniera più dettagliata nei seguenti capitoli), la sostanziale inesistenza di barriere per l'adozione di tali sistemi, sia da parte di attori privati che pubblici, è risultata estremamente minacciosa per il funzionamento degli istituti democratici.

In generale, quindi, la prospettiva vede l'IA invadere sempre più settori, occupando un numero via via maggiore di mestieri di competenza umana. Per ora, essa si ferma all'esecuzione di mansioni di classificazione, spesso legate all'analisi di una grande mole di dati. Le previsioni vedono però questa tecnologia sempre più inclusa nella nostra quotidianità, fino a sostituire l'uomo in professioni ritenute creative o meno "meccaniche".

### - 1.3 L'Intelligenza Artificiale nel contesto geopolitico attuale.

L'IA arriva a determinare l'equilibrio geopolitico mondiale per diverse ragioni, non a caso V.Putin si è espresso a riguardo: "*chi dominerà l'IA, dominerà il mondo*". [1]

L'importanza di tale tecnologia è legata all'impatto economico del mercato dei dati, una buona parte delle principali aziende per capitalizzazione operano infatti in questo settore. È apparso evidente poi, il ruolo di piattaforme come Facebook nella politica interna di alcuni Stati: pensiamo alla campagna elettorale britannica del 2016. [2]

Le quattro grandi compagnie della Silicon Valley (Google, Facebook, Amazon, Apple), sono i principali titolari e sviluppatori dell'IA. Tali imprese raggiungono infatti un valore di 1000 miliardi di dollari ciascuna, [3] a testimonianza appunto di come l'IA rappresenti una fonte di ricchezza smisurata e di conseguenza risulti assai ricercata dagli Stati.

La distribuzione delle tecnologie e delle competenze in materia di IA, si può considerare importante nella determinazione dei rapporti di potere tra gli Stati, al punto da assumere la forma di un nuovo tipo di colonizzazione definita appunto “colonizzazione digitale”.

Come sostiene Cédric Villani, matematico e parlamentare francese, compagnie come Google, Facebook o Alibaba, sono costantemente alla ricerca di nuovi mercati per l'estrazione di dati. In tale ottica si spiegano gli investimenti di tali compagnie in un continente ancora arretrato come l'Africa. Questo tipo di investimenti, può sfruttare la totale assenza o la debolezza delle tutele legali presenti nei paesi occidentali, e ancor di più nei paesi emergenti. Come sostiene appunto Villani, ciò corrisponde ad una vera e propria forma di colonizzazione: *”you exploit a local resource by setting up a system that attracts the value added to your economy. That is what is called cyber-colonization”*. [4]

L'IA quindi risulta e risulterà sempre più decisiva nel determinare il peso geopolitico dei vari paesi, inoltre, come verrà esposto nei capitoli successivi, la concentrazione di potere e di competenze nelle mani di poche compagnie minaccia seriamente la sovranità degli stati [5]. Questi infatti, faticano a bilanciare un'adeguata tutela dei diritti dei propri cittadini, con la necessità di sviluppare strategie competitive a livello geopolitico.

Molti di essi, già da qualche anno, sono impegnati nello sviluppo di tali strategie: attualmente la “corsa all'IA” vede il dominio di Cina e USA, allo stesso tempo la Russia sta cercando di sviluppare tecnologie altrettanto forti.

Altri attori, relegati ad un ruolo secondario, stanno lanciando piani diretti a settori più specifici: l'India si sta concentrando sulla robotica, [6] oppure la Polonia [7] sta ricercando soluzioni innovative nel settore della cybersecurity e nell'impiego militare dell'IA.

Dalle dichiarazioni russe o cinesi si può evincere come l'IA è e sarà nel prossimo futuro l'ago della bilancia nel determinare la potenza egemone: nel Luglio 2017, la Cina ha annunciato la volontà di espandere il volume degli investimenti nel settore, fino ad un valore di \$15,700 miliardi entro il 2030 [8], ed ha inoltre dichiarato di voler diventare l'attore dominante nel settore entro lo stesso anno.

Per realizzare tali obiettivi, sono previsti ingenti investimenti pubblici nelle imprese locali al vertice nel settore. Tale strategia è caratteristica dell' economia cinese, essa prevede infatti

una stretta cooperazione e tra imprese private e vertici del governo.

Ad esempio nel 2017 Alibaba ha investito \$15 miliardi in ricerca sviluppo [9]: un volume di investimenti pressochè eguale a quello di Amazon (16 miliardi) [10].

In risposta la Casa Bianca ha annunciato nel 2018 l'intenzione di mantenere e rafforzare la propria leadership nel settore, concentrandosi nello sviluppo della ricerca.

Gli USA attualmente conservano il proprio primato in virtù del maggiore numero di esperti nell'IA, (quasi doppia rispetto alla concorrenza: “*China has only approximately 39,000 researchers in AI, that is to say, half the American pool of more than 78,000 researchers*”) [11].

In confronto, però, la Cina detiene una mole maggiore di dati: in primo luogo per un bacino di utenza decisamente più largo ed in secondo luogo per l'inesistenza di barriere legali per l'approvvigionamento di dati. Pechino ha inoltre dichiarato di voler incrementare tale colume fino a raggiungere il 30% dei dati globali entro il 2030. Allo stesso tempo la Cina rimane però dipendente dagli Stati Uniti per quanto riguarda i chip ed i processori grafici. la cui potenza è fondamentale nel Machine Learning, o dei principali rami dell'IA.[12]

Per quanto riguarda l'UE, quest'ultima perde terreno nei confronti delle 2 superpotenze. In un report del Senato Francese infatti viene espressa la preoccupazione che il Vecchio Continente possa diventare una “colonia digitale”. L'UE al momento è nettamente indietro negli investimenti nell'IA (“*approximately €2.4 – €3.2 billion in 2016, as compared to €6.5 – €9.7 billion in Asia and €12.1 – €18.6 billion in North America*”) [13], inoltre il settore privato è dominato dalle compagnie Nord Americane a discapito di quelle europee. L'Europa risulta quindi competitiva solo nella formazione delle risorse umane, rimane ancora inespresso il potenziale economico delle aziende europee. [14]

A discapito delle dimensioni degli investimenti, la ricerca accademica riesce a produrre molti talenti, di fatto però resta difficile trattenere questi esperti, che spesso emigrano nella Silicon Valley attirati da opportunità migliori. In più le eccellenze europee emerse finora come la Kuka, (impresa di robotica tedesca, acquistata per 4.5 mlrd USD), difficilmente resistono alle offerte provenienti da Cina o USA.

L'Europa dimostra finora un approccio più cauto nell'impiego dell'IA rispetto alle altre potenze. E' presente dal 2016 il GDPR (General Data Protection Regulation) inoltre con le

successive proposte e raccomandazioni l'UE ha espresso la volontà di regolamentare e sottoporre a dei vincoli tali tecnologie, in modo da tutelare i diritti umani e civili.

Il Vecchio Continente rimane quindi diviso da due obiettivi non facilmente conciliabili: la volontà di competere a livello globale, la quale comporta però la necessità appropriarsi dei dati dei cittadini europei, e la necessità di tutelare i diritti dell'uomo, su tutti la privacy, come annunciato nelle proposte di legge da parte della Commissione Europea.

Al momento la Russia risulta arretrata nello sviluppo dell'IA rispetto a USA e Cina. Indicativo è il numero di start up operanti nel settore: la Russia può contarne solo 193 contro le 8,161 statunitensi e le 1,226 cinesi.[15]

Il Cremlino sta cercando di raggiungere le altre due superpotenze cercando di instaurare una cooperazione tra governo e imprese private o di controllo pubblico. Finora tale consorzio risulta difficoltoso: ad esempio la compagnia russa di spicco (Yandex) nel settore non ha una relazione solida con il governo russo, venendo rilegata ad un ruolo secondario nella Strategia Federale pubblicata nel 2018.

Inoltre la Russia dimostra di essere carente da un punto di vista della coltivazione degli esperti in IA, per di più, come in Europa, molti talenti vengono attirati dai salari assai più elevati delle controparti statunitensi. [16]

In aggiunta, sono carenti gli investimenti nelle tecnologie IA nel settore della difesa, stimati tra i 12 e 36 mln USD, una parte minima rispetto agli investimenti di USA e Cina. [17]

In generale, la Russia fatica a creare un clima economico adatto allo sviluppo di start up, in grado di incentivare gli investimenti di ventura, e di superare le limitazioni imposte dall'autocrazia russa.[18]

Per queste ragioni gli investimenti privati rimangono depressi, impedendo al settore di privato di trainare, come nei casi di Cina e USA, la crescita dell'IA.

A differenza degli USA, dove le grandi corporation dell'high tech hanno sviluppato solo in parte una cooperazione col governo, ma in maniera simile alla Cina, lo sviluppo dell'IA proviene dal governo centrale. Nel 2018 è stata pubblicata la Strategia Federale per l'IA. Questa ha consegnato a Sberbank, considerata la banca privata più importante in Russia, a Rostec (operante nell'industria militare) e Gazprom (il quarto produttore di petrolio al mondo) lo sviluppo di tali tecnologie, in particolare lo sviluppo della rete 5G. [19]

La strategia prevedeva il raggiungimento di 10 obiettivi, tra cui la formazione di un Consorzio nazionale in grado di combinare diversi sforzi, oltre allo sviluppo di un sistema di formazione delle risorse umane. [20] Il piano ha però incontrato diversi ostacoli dovuti all'erogazione dei fondi previsti. Ciò è dovuto in parte alla pandemia COVID-19, nel 2021 il governo ha dovuto revisionare la strategia provvedendo a tagliare parte dei finanziamenti.[21]

*“L’Africa al momento risulta praticamente vergine in termini di infrastrutture digitali”.*

[22]

Al momento la Cina sta intensificando i propri investimenti, già presenti da qualche decennio, in Africa. A livello commerciale la potenza asiatica risulta il maggior partner commerciale nel continente. [23] Come fa sempre notare Morel, l’Africa sta al momento subendo la presenza asfissiante dei cinesi. Nelle telecomunicazioni ad esempio il colosso ZTE provvede a fornire le infrastrutture per il governo etiope, oppure la start-up CloudWalk Technology ha firmato un accordo con il governo dello Zimbabwe per lo sviluppo di tecnologie per il riconoscimento facciale. [24]

Scrivo sempre Nicolas Morel: *“A powerful cyber-colonialist phenomenon is at work here. Still trauma-tized by the liability of European colonization, Africa, confronted with the combined urgencies of development, demography, and the explosion of social inequalities (with which China is quite familiar), is embarking on a logical but very unequal techno-industrial partnership with China.”*[25]

Più recentemente anche Google si è fatta avanti aprendo un proprio centro di ricerca ad Accra, si riscontrano infatti maggiori investimenti occidentali nel settore rispetto al passato. [26]

Al momento quindi l’IA si dimostra uno strumento di potere; sia in ambito militare (con lo sviluppo di droni automatici, o nell’impiego nei servizi d’intelligence), quanto nelle modalità non tradizionali (Soft power), ad esempio tramite l’esportazione di tecnologie o modelli economici, e soprattutto tramite la “colonizzazione digitale”.

## - 1.4 L'Intelligenza Artificiale nella politica interna.

Come già accennato, gran parte della ricerca sull'IA o sulle tecnologie che la rendono possibile provengono dalla ricerca militare. Internet ad esempio nasce nei laboratori di ricerca della DARPA (Defense Advanced Research Projects Agency, l'agenzia governativa statunitense incaricata della ricerca e dello sviluppo dell'arsenale militare), [1] altri progetti più recenti si basano su una stretta cooperazione di agenzie governative e imprese dell'high-tech. [2]

Una più recente e stretta affiliazione è nata infatti in seguito all'incremento delle misure di pubblica sorveglianza, negli USA, ed in Francia e Germania, dopo l'11 Settembre 2001. Definite da S.Zuboff: “Surveillance exceptionalism”, [3] proprio ad indicare il carattere eccezionale e anticostituzionale di tali misure, che ha arrestato le allora incipienti iniziative dirette alla tutela della privacy degli utenti Internet.

La tecnologia che Google aveva iniziato a sviluppare a partire dal 1998, ovvero il motore di ricerca in grado di organizzare le informazioni, ha attirato l'attenzione della CIA. Google ha fornito a quest'ultima la propria collaborazione; ad esempio nell'elaborazione degli algoritmi anti-terrorismo, oppure dotando l'agenzia del dettagliatissimo sistema cartografico denominato Google Maps. [4]

La stretta cooperazione tra Google e le alte sfere della politica statunitense è proseguita con le campagne elettorali di Obama nel 2008 e del 2012. [5] In aggiunta, più recentemente, è emerso il legame tra Facebook e i responsabili di varie campagne elettorali, in particolare la campagna presidenziale americana del 2016 e il referendum sulla Brexit dello stesso anno.[6] Un ex dipendente della società britannica Cambridge Analitica, Chris Wylie, ha rivelato le pratiche illegali che hanno portato all'appropriazione indebita, da parte di Facebook, delle informazioni personali di più di 80 milioni di utenti, il tutto ad insaputa di quest'ultimi. [7]

Il caso risale al 2011, quando un gruppo di ricercatori dell'Università del Maryland annunciò di aver sviluppato un algoritmo in grado di analizzare la personalità degli utenti Twitter,

partendo dalle informazioni divulgate dagli stessi. [8] Tale algoritmo è il culmine delle ricerche nate alla fine degli Anni '90 [9] con lo scopo di applicare all'analisi computerizzata i modelli di valutazione della personalità. [10] Nato all'interno della ricerca medica, lo sviluppo di tali tecnologie, è stato sviato verso le applicazioni in ambito di marketing.

Da allora, infatti, l'ambiente accademico e della ricerca nel campo è stato ampiamente incentivato a tale scopo da colossi come Pepsi. [11] In seguito, con il rapido sviluppo dei servizi derivati dall'IA (come Social Network o piattaforme di E-Commerce), Facebook e Google per prime si sono impegnate nello sviare ricerche di questo tipo, in modo da incrementare l'efficacia degli algoritmi di profilazione. [12]

Nel 2012, Robert Mercer, tra i principali finanziatori della campagna presidenziale di Donald Trump, fonda Cambridge Analitica. [13]

La società nasce con l'intento di sfruttare la mole di dati sensibili di cui Facebook, all'insaputa dei diretti interessati, si è appropriata, “derubando” in tale operazione 80 milioni di utenti. Questi dati, combinati con i modelli predittivi sopra citati, consentivano la produzione di annunci personalizzati, destinati ad influenzare l'esito della campagna presidenziale americana del 2016, e del referendum sulla Brexit del medesimo anno. [14]

Tali esempi dimostrano come l'infiltrazione di grandi corporation nella politica ostacola un'adeguata tutela della privacy, è lampante infatti il conflitto tra l'istituzione di norme a protezione degli utenti e l'estrazione e l'accumulazione delle informazioni personali da parte di società come Google o Facebook. Questi due attori si sono infatti impegnati in un'aggressiva politica contro la regolamentazione del mercato dei dati, fornendo ingenti finanziamenti; ad esempio nelle ultime campagne presidenziali americane. [15]

Non a caso Chris Wylie, ex dipendente di Cambridge Analitica, ha definito il fenomeno di profilazione e approvvigionamento dati “information warfare”, riferendosi alla continua lotta tra i diversi soggetti menzionati (grandi corporation, quanto agenzie di pubblica sicurezza), per l'appropriazione delle informazioni sugli utenti. [16]

Tale dinamica spinge tali compagnie all'occupazione di settori lontani dalla semplice cronologia internet, tale “estrazione” di dati si estende al rilevamento delle informazioni biometriche ottenibili dai dispositivi come orologi da polso intelligenti, dalle applicazioni

utilizzate sugli smartphone, alle informazioni raccolte dalle auto di nuova generazione, e dai robot domestici o televisori. [17]

Questa pervasività è resa possibile dall'onnipresenza dei dispositivi connessi all'“Internet delle cose” (ovvero la rete che permette a diversi oggetti di uso comune come smartphone, elettrodomestici, automobili di collezionare dati e trasmetterli automaticamente comunicando con gli altri dispositivi circostanti). [18]

L'impiego attuale dei Social Network delude quindi le aspettative riguardo al superamento di alcuni ostacoli tipici della vita democratica. Allontanando inoltre la possibilità dei mezzi di telecomunicazione attuali di eliminare i vari filtri, incentivando la partecipazione diretta dei cittadini alla vita politica.

Tali possibilità avrebbero consentito la creazione di una moderna agorà virtuale, in grado appunto di superare la rappresentatività delle cariche politiche, garantendo il dialogo tra i cittadini, grazie alla facoltà di comunicare a grandi distanze.

Uno studio condotto da Javier Martin Reyes [19] sembra piuttosto far intuire il contrario, analizzando la posizioni ideologiche degli americani negli ultimi decenni, si nota una crescente polarizzazione ideologica negli anni più recenti, tale fenomeno si ritiene sia legato alla diffusione ed uso dei social, quale mezzo di espressione ideologica.

Un'analisi attenta sfata le promesse salvifiche legate alla diffusione dei Social Network, oltre alle problematiche legate alla privacy degli utenti (discusse nei capitoli successivi), Reyes dimostra inoltre come tali mezzi di comunicazione accentuino i pregiudizi dei soggetti, disincentivando il dialogo tra ideologie diverse.

Tale dinamica è legata alla logica con i quali sono esposti i messaggi agli utenti, la quale privilegia i contenuti verso i quali si è mostrato apprezzamento. Dal punto di vista ideologico, ciò tende a consolidare le posizioni preesistenti piuttosto che favorire il dialogo.

Da un'analisi dei messaggi provenienti da utenti Twitter o Facebook, emergono infatti diverse tendenze non incoraggianti: in primo luogo i Social incoraggiano l'espressione politica di persone con posizione più estreme rispetto ai partiti di maggioranza (ad esempio i gruppi di estrema destra), rispetto ai soggetti con opinioni politiche intermedie.

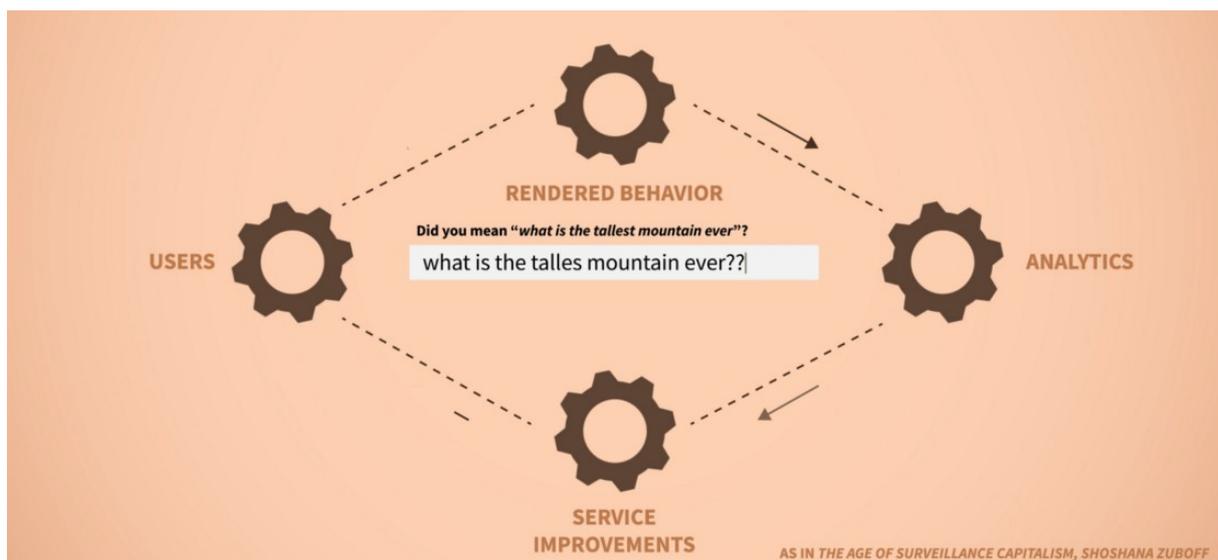
In secondo luogo emerge la scarsità di interazioni tra le persone con posizioni diverse : “più che un agorà virtuale i social network sono una cassa di risonanza”.

Infine i messaggi pubblicati spesso assumono toni più accesi o posizione più estreme rispetto alle interazioni faccia a faccia . [20]

Lo studio analizza le opinioni politiche espresse sulle principali piattaforme di comunicazione (Twitter e Facebook). Personalmente ritengo che tali effetti nefasti siano in parte causati dalla logica intrinseca di tali media. I Social Network menzionati infatti perseguono un profitto basato sull'accumulazione dei dati degli utenti, di conseguenza la logica dietro all'ordine dei contenuti esposti agli utenti ha lo scopo di trattenere quest'ultimi, per il maggior tempo possibile, su tali piattaforme. Favorendo quindi contenuti verso cui l'utente ha espresso gradimento, in modo da poter collezionare un numero maggiore di informazioni. [21] Tale sistema è logicamente incompatibile con gli obiettivi e le speranze legate ad uso benefico delle suddette tecnologie.

### -1.5 “The Age of Surveillance Capitalism”

Il grafico rappresenta il meccanismo descritto nel paragrafo seguente



Per “Surveillance Capitalism” si intende il meccanismo economico descritto da S.Zuboff. L'espressione fa riferimento al circolo di (1) approvvigionamento dei dati degli utenti, (2) di analisi delle informazioni raccolte, le quali in seguito sono (3) tradotte in “prodotti personalizzati” (ad esempi gli annunci pubblicitari personalizzati presenti nei browser). Tali

prodotti sono finalizzati ad un'ulteriore e più precisa raccolta di dati, ed infine (4) esposti nuovamente agli utenti. Tale fase termina il ciclo, il quale proseguirà con una nuova analisi delle informazioni estratte e così via. [1]

Tale ingranaggio è reso possibile dalla concomitanza di diversi fattori (giuridico-politici, tecnologici, socio-economici).

1- La discrepanza tra la rapidità di evoluzione delle tecnologie informatiche rispetto alla normativa di riferimento, citando le parole dell'ex CEO di Intel A. Grove: “*ICT (Information Communication Technologies) goes three times faster than law*”. [2]

Per di più sono presenti numerosi vuoti normativi, che fissino obblighi precisi nei confronti dei fornitori di tali tecnologie, ad esempio determinando particolari obblighi di trasparenza. [3]

2- L'infiltrazione di interessi privati nelle istituzioni democratiche [4], oltre al naturale conflitto, all'interno delle politiche nazionali, tra la necessità di sviluppare delle tecnologie competitive a livello geopolitico e l'obiettivo di garantire la privacy degli utenti.

3- Le possibilità senza precedenti offerte dalle nuove tecnologie: ovvero la capacità di analizzare grandi campioni di dati senza sacrificare la qualità delle analisi. [5]

Gli algoritmi oggi analizzano le informazioni di milioni di utenti, applicando sofisticati modelli psicometrici: ciò sarebbe risultato impossibile per evidenti costi in termini di tempo e risorse prima dell'avvento dei computer.

4- La monopolizzazione del mercato e della ricerca: [6] le grandi corporation della Silicon Valley (Google, Facebook, Apple, Amazon, Microsoft) hanno occupato una fetta consistente di mercato, soffocando la concorrenza tramite l'acquisizione di talenti e start up a prezzi esorbitanti per la concorrenza. Deviando in alcuni casi la ricerca del settore in favore dei profitti economici, piuttosto che verso scopi socialmente utili. Un esempio è il caso della società Realeyes, [7] nata per la creazione di un'interfaccia computerizzata in grado di aiutare soggetti infermi. Questa era originariamente progettata per consentire ai bambini affetti da

autismo, di sviluppare la propria emotività. La start-up è stata più tardi acquistata da Facebook, interessata ai modelli psicometrici, per l'applicazione di tali algoritmi nella profilazione a fini di marketing.

La privatizzazione della ricchezza e delle tecnologie distorce molte delle potenzialità delle varie applicazioni dell'IA: dalla disintermediazione dei mezzi di comunicazione, alla possibilità di innovare la produzione di beni e servizi, alla creazione di strumenti per mitigare il cambiamento climatico.

5- La profonda asimmetria di conoscenza tra i fornitori e gli utenti: come dimostrato precedentemente, l'IA attualmente è incaricata di decisioni importanti quali l'erogazione di mutui ecc. Risulta evidente nonostante la rilevanza di tali decisioni, la distanza tra esperti del settore e gli utenti. Zuboff definisce tale asimmetria “the new priesthood”, in analogia al monopolio dell'interpretazione delle scritture a favore del clero nei secoli del Medioevo. [8]

6- La nebulosità degli algoritmi e la mancanza della necessaria trasparenza:[9]  
l'implicita opacità di molti algoritmi (descritta in seguito nel capitolo 2), ostacola la diffusione di una maggiore conoscenza di essi; allo stesso tempo risultano assenti gli sforzi da parte dei fornitori di tali servizi per rendere più comprensibili e trasparenti tali tecnologie. Strumenti come LIME [10] (capitolo 2) possono agevolare tale compito di per sé già difficile. Dal punto di vista legislativo la normativa presente risulta troppo vaga, limitandosi a fissare principi generali senza elaborare obblighi specifici ed adeguati alla situazione. [11] (capitolo 3)

La nuova economia digitale ha creato profonde diseguaglianze nella distribuzione del sapere: Zuboff descrive l'asimmetria di informazioni tra i padroni delle informazioni digitali e gli utenti equiparandola alla conquista spagnola dell'America del Sud a spese degli impotenti indigeni americani [12]. Allora i conquistadores dichiararono in nome della fede e della corona di Spagna la sovranità dei territori indigeni. Nel XXI sec. Google asserisce a sé il diritto allo sfruttamento dei dati provenienti dagli utenti. La pervasività dei dispositivi

tecnologici ha reso possibile una profilazione estremamente dettagliata, [13] simile ad una vera e propria distopia.

Tale asimmetria è causata da una bassa distribuzione delle conoscenze digitali. Le grandi corporation assumono gran parte dei laureati nel settore; oltre a ciò mancano investimenti nella riqualificazione di molti lavoratori. Molte aziende preferiscono infatti automatizzare una determinata mansione, che spesso va a sostituire le professioni che necessitano di una media specializzazione (middle skilled jobs), come ad esempio i lavori di sportello. La domanda di lavoro si concentra quindi più in settori con mano d'opera non specializzata, spesso retribuita con salari minimi, e in mano d'opera assai qualificata e ben retribuita. [14]

La recente digitalizzazione, piuttosto che portare ad un coinvolgimento nella vita democratica, ha di fatto agevolato enormi concentrazioni di potere, ha depauperato gli utenti dei servizi digitali delle più elementari forme di privacy, oltre ad instaurare subdoli metodi di controllo basati su metodi psicometrici e di stimolo per condizionare scelte politiche o indurre al consumo di prodotti. [15]

Google impiega diverse delle tecnologie definite IA, tra cui: la produzione di algoritmi “classici”, l'analisi predittive, o l'apprendimento automatico. (Google 2018) [16]

Sono proprio tali algoritmi i “mezzi di produzione”, per usare la terminologia di Marx, gli strumenti in grado di convertire i dati collezionati in previsioni dei futuri comportamenti degli utenti.[17]

Sempre Zuboff fa notare la particolarità del capitalismo di sorveglianza: grazie agli algoritmi viene eliminata la tensione tra quantità e qualità tipica del modello industriale precedente, infatti l'efficacia di tali algoritmi aumenta con la mole di dati con quale questi sono “nutriti”. [18]

Un esempio della portata di tali tecnologie è rivelato da un report del team di Bing (il motore di ricerca di Microsoft), il quale segnala che un aumento dello 0,1% dell'accuratezza nella stima delle visualizzazioni di una pubblicità, risulterebbe in centinaio di milioni di dollari di ricavo. (Microsoft 2017) [19]

“The Age of Surveillance Capitalism” riporta il modo vorace in cui le grandi imprese dell'hightech (Google su tutti), si sono espanse allargandosi su tutti i fronti per garantirsi un approvvigionamento sempre maggiore di dati, ad esempio acquistando a cifre apparentemente spropositate piccole imprese emergenti.

E' il caso ad esempio di Youtube, [20] acquistata nel 2006 per ben 1,65 miliardi di dollari, “la start up aveva solo un anno e mezzo di vita non aveva ancora creato utili ed era stata denunciata per violazione di copyright”, altro caso è quello di Oculus Rift, [21] acquistata da Facebook per 2 miliardi USD, prezzo considerato astronomico dagli esperti.

Zuboff fa notare inoltre come la pervasività di tale economia si sia spinta verso i confini estremi della privacy individuale, violando il consenso e operando in maniera subdola, inglobando e monopolizzando sempre più tecnologie in cerca di nuove fonti di dati, senza nessuna cura per gli spazi personali degli utenti. [23]

Ad esempio nel settore degli assistenti digitali le grandi compagnie si sono impegnate a fondo nel creare algoritmi in grado di riconoscere il linguaggio umano, in modo da poter trasformare i miliardi di file audio, messaggi vocali o conversazioni catturare dagli ubiqui dispositivi internet, in informazioni rivendibili a fini di marketing. [24]

Spacciando tali violazioni come “personalizzazioni”, [25] tali imprese si sono spinte verso una sempre più profonda incursione nelle sfere personali degli utenti, che ignari condividevano un numero di informazioni crescente, il quale si trasformava in seguito in pubblicità ancor più mirate in grado di raccogliere ancor più dati, innescando così il circolo vizioso descritto ad inizio capitolo.[26]

La start up Realeyes dal 2015 ha sviluppato un progetto per la profilazione emotiva, con l'obiettivo di programmare un algoritmo in grado di riconoscere il linguaggio corporale o non verbale (voci, gesti, espressioni). Tali piccoli fenomeni infatti avvengono in maniera inconscia ad esempio quando conversiamo con altri e rivelano in maniera molto più profonda rispetto al linguaggio le nostre emozioni o le nostre intenzioni. [27]

Come espresso in precedenza, dagli anni 60's vengono elaborati modelli per la codificazione del linguaggio verbale: ad esempio FACS, modello elaborato da Paul Ekman, classifica le emozioni in base alle espressioni facciali, consentendo la creazione di nessi causali tra espressioni ed emozioni.

Rosalind Picard negli anni 90' riconosce la validità del modello di Ekman e inizia a sviluppare l'idea di poter adattare tale modello ad un sistema computazionale.

L'obiettivo era quello di creare un computer intelligente in grado di rispondere ai bisogni affettivi di un paziente, con l'intento di aiutare delle persone in difficoltà, ad esempio affiancando i bambini autistici nello sviluppare la propria emotività. [28] Il modello doveva adattarsi alle esigenze e peculiarità del paziente/utente, ciò grazie appunto alle tecniche sopra menzionate. Picard sottolineò anche la necessità di preservare la privacy degli utenti facendo riferimento alla delicatezza delle informazioni catalogate. [29]

Al giorno d'oggi tale idea si è effettivamente realizzata, allo stesso tempo si sono però avverate le preoccupazioni della Picard riguardo alla privacy. Negli ultimi anni il mercato definito dei “computer affettivi” è cresciuto dai 9 miliardi USD del 2015 fino ai 54 miliardi del 2021 [30], tale impiego nonché impulso rimane però concentrato nel sviluppare tecniche di profilazione ai fini di marketing.

Gli algoritmi come quelli sviluppati dalla Realeyes sono particolarmente pericolosi: impiegando sottili tecniche e modelli psicologici su larga scala consentendo una precisa mappatura psicologica di un individuo, e questo pone serie questioni etiche sulla privacy e sull'impiego di tali sistemi in ambito di pubblica sicurezza. Finora la normativa europea lascia molte riserve sull'impiego di tali sistemi, il quale risulta ancora largamente consentito.

Rimane quindi sostanziale il gap tra i possibili usi virtuosi dell'IA e le applicazioni più comuni di tali tecnologie, L'informatico J. Weizenbaum pone l'accento sulla superficialità con la quale molte tecnologie vengono impiegate senza particolari riflessioni sugli effetti lesivi che potrebbero creare o sulle stesse destinazioni: *“One can't escape this state without asking, again and again: What do I actually do? What is the final application and use of the products of my work? and ultimately, “Am I content or ashamed to have contributed to this use?”* [31]

In altri settori Apple, Google, e Amazon stanno espandendo le loro reti alla ricerca di nuovi profitti, sempre a tale scopo infatti hanno stretto accordi con diversi produttori d'auto per l'inclusione dei dispositivi di riconoscimento vocale all'interno di vari modelli di automobili. [31]

Inoltre, per le stesse ragioni è stato finanziato lo sviluppo dei sistemi di identificazione biometrica: dal 2010 l'Università del Maryland ha dimostrato di poter programmare degli

algoritmi in grado di fornire un'analisi della personalità partendo dalle informazioni condivise dagli utenti Facebook.

Nel 2016 il CEO di Microsoft Satya Nadella dichiara a proposito del nuovo assistente digitale dell'azienda Cortana: *“It knows you deeply. It knows your context, your family, your work. It knows the world. It is unbounded. In other words, it’s about you; it’s not about any one device. It goes wherever you go.”* [32]

La semplice profilazione, si è poi evoluta nella creazione di veri e propri sistemi per il condizionamento del comportamento degli utenti, lo scandalo di Cambridge Analytica ha fatto emergere l'uso a scopo politico di tali sistemi.

*“It's no longer about ubiquitous computing. Now the real aim is ubiquitous intervention.”* [33]

A tale fine Google ha investito ingenti risorse nello svolgere esperimenti allo scopo di monitorare le reazioni degli utenti a diversi layout o opzioni; tali esperimenti hanno lo scopo di fornire previsioni riguardo ai futuri comportamenti degli utenti in maniera tale da migliorare gli algoritmi. [34]

Come fa notare Zuboff per approssimarsi alla certezza è necessario svolgere per l'IA il numero più alto possibile di esperimenti; gli algoritmi sono infatti in grado di svolgere un numero enorme di esperimenti autonomamente, superando quindi i limiti della sperimentazione “analogica”.

La capacità di questi sistemi arriva inoltre ad eludere la consapevolezza degli utenti: *“methods that bypass human awareness, individual decision right, and the entire complex of self-regulatory process that we summarize with terms such as autonomy and self-determination”*[35].

Un esperimento condotto da Facebook durante le elezioni americane mid-term del 2010, consisteva nel mostrare ad un gruppo di utenti quali dei loro conoscenti (amici) avesse dichiarato di votare, ad un secondo gruppo invece tale informazione non veniva mostrata. Il risultato rivela che gli utenti del primo gruppo erano più propensi a dichiarare loro stessi di aver votato (il 2% in più); rispetto all'altro gruppo.

I ricercatori, alla luce di tali risultati, hanno concluso che tale messaggio avesse poi realmente influenzato l'effettiva partecipazione al voto. Si suppone che tale esperimento abbia portato

fino a 340,000 voti addizionali, voti (viste le ultime elezioni, soprattutto negli USA) potenzialmente determinanti. [36]

In un altro esperimento, sempre condotto da Facebook, venivano manipolati i contenuti mostrati sui vari profili della piattaforma.

L'obiettivo della ricerca consisteva nel dimostrare qualora gli utenti del Social Network avrebbero in seguito postato dei messaggi che riflettersero il tono dei contenuti che venivano loro mostrati.

I numerosi esperimenti condotti da Facebook sono stati segnalati per le numerose violazioni della normativa previste nel campo della ricerca scientifica. In un report del Wall Street Journal vengono evidenziate le ripetute violazioni di tali normative. L'articolo riporta che il gruppo di ricerca ha sostenuto dal 2007 più di 1000 esperimenti di tale genere, senza la minima sorveglianza o rispetto dei criteri dettati per le ricerche di questo tipo. [37]

In maniera simile ai casi già citati, in un report sempre di Facebook del 2017, basato sull'analisi psicologica di 6,4 milioni di australiani, tra cui molti studenti, viene citato il modo in cui la compagnia, monitorando l'attività degli utenti, possa determinarne lo stato d'animo e in più sfruttare determinati stati in cui gli utenti risultano più vulnerabili, per sottoporre questi all'esposizione di studiate configurazioni pubblicitarie. [38]

## 1.6 Intelligenza Artificiale e ambiente.

Un altro aspetto di cui è necessario tener conto, nella pianificazione delle politiche in materia di IA, è sicuramente l'impatto ambientale di tale tecnologia. L'IA non è ecologica, con l'aggravarsi dei cambiamenti climatici diventa sempre più necessario contingentare le risorse energetiche; dev'essere quindi discusso l'impatto di questo strumento.

Se da un lato l'IA risulta utile nel contenere in cambiamento climatico, permettendo ad esempio di monitorare in maniera più accurata il clima, [1] d'altro canto essa necessita di enormi quantità di energia per processare l'enorme volume di dati immessi [2]. I dati come spiegato nei capitoli precedenti rappresentano il “carburante” di queste macchine.

L'IA viene presentata come una tecnologia ecologica, Google e Apple ad esempio dichiarano di essere “carbon neutral,” ovvero in equilibrio tra le emissioni e l'assorbimento di carbonio, la prima inoltre dichiara che sarà indipendente dai combustibili fossili dal 2030. [3]

In realtà risulta difficile determinare il peso specifico delle emissioni prodotte dall'IA.

Rimane invece più pratico stabilire il peso delle tecnologie “ICT” (Information Communication Technologies) in generale, dato appunto che spesso l'IA è combinata ad altre tecnologie come internet. A tal proposito si calcola che le emissioni delle tecnologie di telecomunicazione in generale raggiungerà il 14% delle emissioni globali nel 2040 [4]. Inoltre è ragionevole pensare che il prevedibile sviluppo dell'Intelligenza Artificiale occuperà una fetta maggiore delle tecnologie ICT in futuro e che quindi l'IA contribuirà in maniera più consistente alle emissioni nei prossimi anni. [5] Per dare un'idea dei consumi richiesti per “l'apprendimento” dei sofisticati modelli per l'analisi del linguaggio naturale (utilizzati da compagnie come Google), questi possono raggiungere i 300,000 kg di CO<sub>2</sub>, equivalenti a 125 voli andata e ritorno da New York a Pechino. [6]

Come fa notare inoltre Nordgren tale consumo è relativo al solo allenamento e non è indicativo del consumo del modello nel “mondo reale”. [7]

Bisogna poi considerare l'effetto “rebound” (rimbalzo in inglese), ovvero considerare tutte le emissioni indirette provenienti da una tecnologia come l'IA.

Di fatto il prevedibile miglioramento nell'efficienza dell'IA potrebbe condurre al paradosso di Javon (1835-1882), ovvero una maggiore efficienza energetica in un settore, potrebbe

paradossalmente portare all'aumento delle emissioni. Ad esempio la produzione di automobili meno inquinanti, si è tradotta in un aumento delle auto circolanti e quindi di fatto in maggiori consumi (direct rebound). Ciò in seguito ha generato una maggiore domanda e consumo di prodotti complementari alla tecnologia principale (nel caso delle auto, un esempio sono gli pneumatici), che a sua volta ha portato alla crescita della domanda di servizi indirettamente connessi alla tecnologia originaria (sempre nell'esempio delle auto: alberghi o strutture turistiche). Quanto descritto ha portato infine alla creazione di una vera e propria economia derivata o comunque connessa al mercato originario. Nel caso dell'IA, il miglioramento dei modelli attuali si tradurrebbe probabilmente in maggiore richiesta e quindi in un maggiore numero di applicazioni, e quindi in maggiori emissioni (Nordgren). [8]

E' necessario poi considerare tra gli effetti indiretti i costi ambientali di estrazione delle materie prime, il trasporto di questi, oltre al consumo energetico nella trasformazione in prodotti finiti. [9]

L'IA allo stesso tempo può contribuire a contenere o mitigare il cambiamento climatico in diverse maniere [10], ad esempio tramite la limitazione dei consumi (nel caso dell'IA si dovrebbe restringere la mole di dati processabili, in analogia con le restrizioni sul consumo delle auto), oppure attraverso la limitazione di questa nei servizi considerati accessori come servizi di lusso o d'intrattenimento.

Al di là della riduzione delle emissioni di questa tecnologia, l'Intelligenza artificiale può contribuire alla mitigazione climatica attraverso il monitoraggio delle risorse ambientali, attraverso la creazione di edifici o intere città più efficienti. Oltre a ciò, è possibile grazie ad essa, ottenere materiali sintetici più ecologici, migliorare il design o la resistenza di tecnologie già esistenti, oppure prevedere eventi climatici estremi. [11]

Nordgren menziona inoltre la possibilità da parte delle istituzioni di utilizzare l'IA nello spronare o influenzare i comportamenti degli utenti verso scelte più ecologiche [12]. In sé tale applicazione può agevolare una mitigazione del clima, ma allo stesso tempo implica serie minacce alla privacy e al riserbo degli utenti, infatti finora tecnologie di sorveglianza simili sono utilizzate per sfruttare a scopi di marketing i dati raccolti sugli utenti (si veda capitolo precedente). Tale opzione dev'essere valutata con estrema attenzione, ad ora infatti non sono

presenti delle tutele adeguate che rendano tali tecnologie compatibili con i diritti umani e civili.

In relazione alle possibili applicazioni sopra elencate, considerato inoltre la prevedibile necessità di contingentare il consumo energetico, diventa importante dal punto di vista di diversi attori come policy-maker o privati, investire nelle tecnologia con i prospetti migliori. [13]

Rolnick e colleghi [14] hanno proposto una possibile selezione delle applicazioni del machine learning, una delle tecnologie principali dell'IA, basata sulla classificazione dei probabili impatti di ciascun impiego.

Tale criterio privilegierebbe le tecnologie che nell'immediato possono alleggerire le emissioni, rispetto ad altre tecnologie che potrebbero rivelarsi più utili in questo senso; ma che necessitano di maggiore sviluppo, come la fusione nucleare o la geo-ingegneria.

Infine relegate ad un impiego eventuale sono le applicazioni ad esito incerto ovvero che potrebbero generare effetti secondari nocivi, come descritto nel paradosso di Javon. [15]

Tale modello si basa però sulle informazioni attuali in possesso, secondo cui alcune tecnologie potrebbero non rispettare le attese, ad esempio l'IA impiegata nel design di edifici ecologici potrebbe non essere abbastanza efficiente da colmare i consumi del suo impiego, o altrimenti potrebbero emergere effetti secondari non previsti. A tale scopo quindi è necessario adeguare tali politiche alle future eventualità. [16]

Risulta quindi ancora difficile definire il reale impatto ambientale dell'IA. Alcuni studiosi si rivelano fiduciosi in tal senso, mentre altri suggeriscono una maggiore riduzione del loro impiego. Tali previsioni infatti devono tenere in conto della attesa evoluzione tecnologica, che potrebbe risultare onerosa in termini di emissioni, in un primo periodo, salvo magari permettere di trovare soluzioni efficaci in un secondo periodo. [17]

Eventuali misure restrittive riguardo all'impiego dell'IA potrebbero indirettamente limitare la libertà individuale, [18] impedendo l'accesso ad un numero sempre più elevato di servizi. Ormai da qualche decennio infatti molti di questi sono digitali; è quindi un compito assai delicato stabilire quali risorse debbano essere limitate ed in quale modo.

Misure troppo restrittive potrebbero stabilire una sorta di controllo autoritario tale da restringere effettivamente la libertà individuale, ugualmente, la mancanza di intervento risulterebbe irresponsabile e catastrofica.

Allo stesso modo l'utilizzo da parte delle istituzioni di sistemi di condizionamento a scopi umanitari, menzionato da Nordgren, risulterebbe praticamente incompatibile con il rispetto dei diritti personali, e sfocerebbe molto probabilmente in una moderna distopia; le esperienze attuali di sorveglianza si sono finora così rivelate (vedi capitolo precedente).

Si pone inoltre il problema di come la riduzione delle emissioni possa rimanere compatibile con la diffusione di tali tecnologie nei paesi in via di sviluppo [19], il che già di per sé decuplicherebbe il numero di utenti che utilizzano tecnologia IA. In secondo luogo è prevedibile che in tali paesi risulti ancor più complicato, rispetto alle nazioni sviluppate, imporre tutele adeguate.

L'esigenza di controllare la produzione e l'impiego di tecnologie intelligenti comporta la necessità di determinare gli obblighi degli attori maggiormente responsabili dei consumi. Autori come Malliaraki [20] considerano una delle soluzioni imporre maggiori obblighi nei confronti delle compagnie produttrici e fornitrici dei servizi IA, stabilendo inoltre dei doveri di trasparenza riguardo alle emissioni prodotte durante l'apprendimento e uso dei modelli. Parimenti è necessario un adeguato impulso normativo, che stabilisca obblighi di trasparenza in termini di emissioni e non solo.

Gailhofer suggerisce ad esempio delle politiche ambientali che delimitino la quantità dei dati accumulati: *“the goals of AI systems are not only integrated by design in line with the intention of the producers, but also develop automatically and dynamically based on data. Thus, regulation must specifically also take into account the data used to train AI.* [21]

Allo stesso modo sarebbe utile cercare di prevedere e anticipare, all'interno delle politiche ambientali, gli effetti indiretti provenienti dalle varie tecnologie IA.

Sempre Gailhofer fa notare come nell'atto unico sull'IA (si veda capitolo 3) non sia direttamente menzionato la regolamentazione dal punto di vista ambientale. Il testo infatti si concentra esclusivamente sulla tutela degli utenti, sicuramente si dovrebbe implementare tale aspetto, visto il cambiamento climatico attuale una parte dedicata all'ambiente. [22]

E' opportuno segnalare inoltre l'importanza di provvedere, con adeguate politiche ,alla regolamentazione dell'uso dei dati, come esposto nei capitoli precedenti. Questi rappresentano una preziosa moneta di scambio. Organizzare e stabilire un opportuno controllo sull'accesso ai dati, privilegiando attività virtuose o ecologiche può garantire un uso più etico dell'IA, limitando inoltre gli abusi della privacy degli utenti.

Un controllo accurato, unito all'utilizzo di tecnologie affidabili ed eticamente rispettose, potrebbe garantire una maggiore fiducia degli utenti verso l'IA. Inoltre un efficiente sistema di accesso ai dati raccolti da parte di essi come previsto dal GDPR potrebbe consentire una più fruttuosa interazione tra utenti, policy maker e privati, agevolando lo sviluppo di un IA migliore.

E' inoltre auspicabile la costituzione di un “passaporto digitale” in grado di fornire informazioni circa l'origine, la scadenza, la composizione, le possibilità di riciclaggio ecc. dei prodotti digitali. [23]

Si segnala in aggiunta il progetto “*Destination Earth*”, [24] il quale contiene diverse iniziative rivolte alla creazione di un sistema di monitoraggio delle condizioni climatiche e delle attività umane sul pianeta. Tale progetto contiene diversi obiettivi tra i quali:

*“the review of the regulatory framework for interoperable data-sharing in rail transport in 2022; in the energy sector: actions for improving the interoperability in smart buildings and products, actions to improve their energy efficiency, optimise local consumption and broaden the integration of renewable energy sources”*. Inoltre è prevista l'erogazione di investimenti nel settore agricolo, in modo da sfruttare il potenziale delle tecnologie IA, ponendo particolare attenzione verso le aree rurali.

Infine la recente Strategia Europea sui Dati (si veda capitolo 3) ha annunciato l'intenzione di regolamentare i seguenti settori:

- *the Ecodesign Regulation on servers and data storage products;*

• *the EU Code of Conduct on Data Centre Energy Efficiency;*

• *the EU Green Public Procurement criteria for data centres, server rooms and cloud services;*

• *the Energy Efficiency Directive.* [25]

## Capitolo Secondo

### **Analisi delle problematiche legate all'uso dell'Intelligenza Artificiale.**

*“Un **modello black box** è un sistema che, similmente ad una scatola nera, è descrivibile essenzialmente nel suo comportamento esterno ovvero solo per come reagisce in uscita (output) a una determinata sollecitazione in ingresso (input), ma il cui funzionamento interno è non visibile o ignoto “.* [1]

Diversi algoritmi operanti nel mondo reale sono “*scatole nere*”. Finora si è posta molta attenzione sulle prestazioni dei modelli; questi si occupano di scoprire le correlazioni più frequenti, in relazione ad un certo obiettivo, spesso trascurando però una spiegazione causale dietro ogni scelta. [2]

Visto il crescente sviluppo ed impiego di tali tecnologie è logico ipotizzare che l'IA negli anni a venire sarà responsabile di decisioni ancor più rilevanti. (si vedano capitoli 1.2, 1.3)

Finora l'impiego dell'IA si è rivelato non scevro da problemi, data infatti l'autonomia con cui l'algoritmo determina le proprie decisioni, può risultare complicato persino per gli stessi autori dell'algoritmo comprendere i motivi di una determinata decisione dell'IA. Oltre a ciò questa può funzionare diversamente a seconda dei contesti, l'operato può variare in ambiente protetto (come avviene durante la fase di sviluppo), rispetto all'operare nell'ambiente reale, ove la macchina può essere sottoposta a input non previsti o prevedibili. [3] Casi del genere pongono questioni sull'affidabilità di tali algoritmi, rendendo necessaria la possibilità di tutelarsi da parte dei diretti interessati nei confronti delle decisioni dello stesso. Si pensi specialmente a casi delicati come la diagnosi di una malattia o l'imposizione di misure restrittive verso libertà personale di un individuo. Anche gli input determinabili dall'uomo devono essere chiari e vincolati al rispetto di determinati principi legali. In particolare risulta necessario evitare di riprodurre nell'algoritmo eventuali pregiudizi umani: ad esempio un algoritmo basato su pregiudizi razziali non farà che riprodurre o accentuare tali pregiudizi.

Inoltre risulta fondamentale introdurre specifici obblighi in maniera da poter determinare in caso di incidenti o irregolarità, le responsabilità dell'accaduto. Pensiamo ad esempio ad un sinistro stradale causato da un'auto a guida autonoma. Un'adeguata trasparenza consentirebbe

di evidenziare i potenziali elementi irregolari nell'algoritmo, consentendo quindi di determinare la responsabilità dei programmatori dell'algoritmo e di garantire giustizia. E' dunque necessario regolamentare l'IA, in modo da contenere e possibilmente anticipare i rischi provenienti dai futuri sviluppi di quest'ultima; oltre a sviluppare mezzi che agevolino tale controllo come l'algoritmo LIME.

Secondo Burrell (2016) [4] esistono quindi 3 barriere che impediscono la creazione di un IA trasparente:

- 1) Le decisioni rilevanti sull'IA sono riservate alle grandi corporation, le restanti decisioni prese a livello istituzionale sono lontane dallo scrutinio pubblico.
- 2) Il gap nell'istruzione digitale: poche persone, rispetto al numero totale di utenti, sono in grado di comprendere una linea di codice. Tale capacità inoltre non è sempre sufficiente a capire il funzionamento globale di un modello.
- 3) Difetto nella progettazione: con attenzione quasi completamente rivolta alle performance del modello. D'altro canto sono trascurati requisiti importanti come l'interpretabilità o la comprensibilità da parte di un utente umano.

Nonostante le migliori intenzioni, rendere comprensibili algoritmi complessi può risultare molto difficile o non realizzabile completamente: come spiegano gli autori di LIME (si veda capitolo 2.1), spesso ci si trova davanti ad un trade-off tra l'accuratezza della spiegazione e la sua comprensibilità. In altre parole alcuni algoritmi utilizzano correlazioni troppo complesse per essere rappresentati fedelmente da una rappresentazione lineare (ad esempio il grafico usato da LIME).[5]

Sarebbe opportuno quindi che fossero introdotte norme che vincolino la progettazione di questi algoritmi a dei requisiti di trasparenza e interpretabilità. Ciò che è stato fatto finora nel contesto europeo, manca della necessaria accuratezza, non sono per ora definiti standard precisi e inequivocabili a tal proposito (come espresso nel capitolo seguente), né è presente un organismo imparziale in grado di garantire un'adeguata sorveglianza sulla progettazione e impiego di tali modelli.

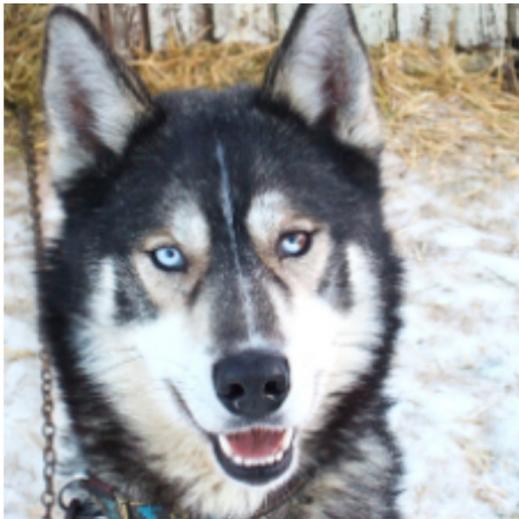
## 2.1- Il modello LIME

La capacità di comprendere e di poter constatare l'affidabilità di un algoritmo è cruciale. Tale compito può essere reso possibile attraverso appositi modelli in grado di risalire ai fattori determinanti nell'elaborazione dell'output. L'algoritmo LIME sviluppato da Ribeiro, Singh e Guestrin è in grado di mostrare graficamente i fattori rilevanti in maniera comprensibile anche ai non esperti. [6] Il modello consente di rilevare i fattori determinanti in un singolo risultato, infatti, data l'imperscrutabilità degli algoritmi black box è spesso impossibile o molto complicato arrivare a ricostruire globalmente l'algoritmo. LIME permette però di rendere comprensibile la funzione a livello "locale" [7], ovvero il responso dell'algoritmo in situazioni simili a quella analizzata. Come ammesso dagli autori, il modello si scontra con i limiti dati dalla possibilità effettiva di rappresentare efficacemente un algoritmo. Talvolta infatti non è possibile semplificare in maniera comprensibile una funzione. [8]

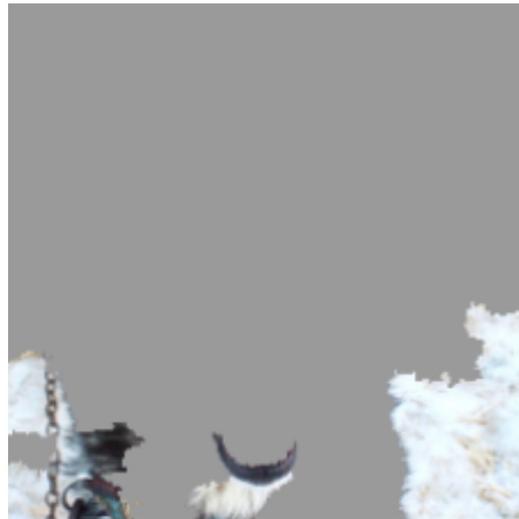
Ad esempio, nel caso di un algoritmo di diagnosi, la capacità di esplicitare i fattori determinanti e il loro peso relativo, permetterebbe di testare la precisione del modello e di correggerne gli eventuali difetti.[9]

A dimostrazione dell'importanza di tale questione, i ricercatori hanno condotto un esperimento per testare la capacità di un esperto in materia di riconoscere gli errori di un modello. Mostrando ai soggetti un algoritmo con una correlazione volutamente fuorviata, ed in seguito domandando loro qualora l'algoritmo fosse affidabile o meno. L'esperimento mostra la difficoltà con la quale, persino un esperto, messo al corrente di potenziali errori nell'algoritmo lo consideri affidabile. All'algoritmo venivano mostrate immagini di lupi selvatici e di cani Huski [10], il modello "nutrito" con immagini di Huski e di Lupi doveva distinguere i due tipi. La rete neurale doveva elaborare autonomamente le correlazioni che gli avrebbero consentito di distinguere le due categorie. Sebbene apparentemente accurato, la distinzione tra le due categorie veniva determinata dalla presenza/assenza di neve nella foto, infatti nelle immagini contenenti dei lupi era quasi sempre presente della neve sullo sfondo. Da questo esempio emerge inoltre come i criteri che oggettivamente distinguono il lupo dall'Huski ovvero il colore della pelliccia, gli occhi, o la forma delle orecchie e del muso sono

irrilevanti per l'elaborazione del risultato, il quale veniva determinato da un elemento insignificante. [11]



(a) Husky classified as wolf



(b) Explanation

Modelli come LIME possono agevolare la comprensione degli algoritmi anche da parte di utenti non esperti. Mostrando graficamente i fattori determinanti si può facilmente risalire al processo decisionale del modello analizzato, come ad esempio nel grafico sopra riportato, relativo al summenzionato algoritmo Huski- Lupo.

Al di fuori del modello LIME, il quale si occupa degli algoritmi di classificazione, rimane opportuno studiare ed imporre apposite misure in tutte le applicazioni dell'IA.

Come espresso nell'introduzione, all'interno della definizione di IA sono inserite tecnologie molto diverse fra loro, le quali necessitano di conseguenza di misure specifiche circa il loro uso.

Sebbene da un punto di vista legislativo risulti opportuno assimilare tutte le tecnologie IA in un testo unico, dal lato tecnico è richiesta un'attenzione dettagliata per ogni singola tecnologia.

Le auto a guida autonoma ad esempio potrebbero incorporare nei loro algoritmi un modello fungente scatola nera, analogamente agli aerei di linea. Tale modello dovrebbe idealmente rispettare dei requisiti tecnici specifici, quale ad esempio: la possibilità di accedere ai fattori determinanti la decisione dell'algoritmo. In aggiunta, sarebbe opportuno imporre alle aziende

sviluppatrici di tecnologie IA, di fornire un report dettagliato del comportamento di questa, sia in fase di collaudo, che nel “mondo reale”.

Garantendo quindi la possibilità di ricostruire in maniera agevole il processo decisionale dell’ algoritmo.

Gli strumenti di trasparenza dovrebbero infine risultare il più possibile accessibili ad un utente medio. Come esposto nell’esempio di LIME, la progettazione degli strumenti di controllo risulta particolarmente impegnativa, per via della complessità degli algoritmi analizzati.

La possibilità di sorvegliare le decisioni dell’IA, deve però essere il più possibile considerata, in maniera da concedere la possibilità autotutela da parte degli utenti, ed assicurare una maggiore democraticità ed utilità di queste tecnologie.

## Capitolo Terzo

### **La normativa vigente nell'Unione Europa e le politiche attuali in materia.**

Sebbene l'Europa al momento sia decisamente arretrata rispetto a USA e Cina nello sviluppo e negli investimenti in tali tecnologie (4 mlrd USD rispetto agli 8-12 dell'Asia e 15-23 mlrd in Nord America) [1], essa è pioniera nella regolamentazione dell'IA. A partire dal 2016 con la pubblicazione del GDPR (General Data Protection Regulation), primo regolamento a regolamentare alcuni aspetti gli algoritmi “black box”[2], l'UE ha in seguito proseguito la stesura di un testo contenente delle “linee guida etiche”. Ad esso sono seguiti diversi documenti sino all'attuale proposta di regolamento

Attualmente l'UE dichiara tra i suoi obiettivi lo sviluppo dell'IA nel rispetto dei suoi valori, nel rispetto della dignità umana. [3]

Storicamente, il diritto alla privacy risale al 1950, nella Convenzione europea sui diritti umani viene infatti menzionato il diritto al riserbo e alla vita familiare. [4]

In seguito la Direttiva madre nel 1995 [5] unifica la normativa sulla privacy, fin quindi frammentata a livello nazionale (ovvero richiedeva l'approvazione tramite leggi nazionali) con attenzione verso il trattamento dei dati e che fissa esplicitamente il diritto alla protezione dei dati sensibili.

In seguito nel trattato di Lisbona tale diritto acquista lo status di diritto fondamentale dei cittadini dell'UE. [6]

Il GDPR, pubblicato nel 2016, nasce con lo scopo di armonizzare definitivamente le normative vigenti nell'unione. Il regolamento inoltre stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei loro dati personali. [7]

Questo inoltre introduce regole più chiare in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, stabilisce alcuni criteri per il trasferimento dei dati al di fuori dell'Ue e per i casi di violazione dei dati personali. [8]

Rispetto alla normativa precedente è importante sottolineare il superamento della dimensione territoriale del trattamento dati: visto infatti che questo spesso avviene al di fuori dell'Ue.

Viene stabilito infatti il rispetto della normativa europea anche nei casi in cui il trattamento avviene al di fuori della stessa. [9]

Viene inoltre posta particolare attenzione alla dimensione tecnologica nei principi “*Privacy by default, privacy by design*”: il primo impone ad un sistema o servizio di utilizzare nel trattamento dati le misure più favorevoli alla privacy degli utenti; il secondo principio (by design) prescrive ai fornitori di tecnologie legate all'uso di dati di considerare e implementare, a partire dal design del prodotto/servizio delle misure che proteggano la privacy dei soggetti. [10]

In generale, le nuove norme prevedono, inoltre:

- (1) per i cittadini un più facile accesso alle informazioni riguardanti i loro dati e le finalità e modalità di trattamento degli stessi;
- (2) un diritto alla portabilità dei dati che consente di trasferire i dati personali da un sistema di trattamento elettronico ad un altro;
- (3) l'istituzionalizzazione del diritto all'oblio (denominato diritto alla cancellazione nel Regolamento), come previsto dalla Corte di Giustizia europea, che consentirà di chiedere ed ottenere la rimozione dei dati quando viene meno l'interesse pubblico alla notizia;
- (4) sanzioni amministrative fino al 4% del fatturato globale delle aziende in caso di violazioni delle norme. [10]

Il testo definisce inoltre le forme a tutela dei singoli utenti: nell'articolo 17 ad esempio viene definito il diritto alla cancellazione dei dati. [11]

Di particolare importanza è l'articolo 22, [12] il quale stabilisce il diritto da parte degli utenti a non essere sottoposti a decisioni provenienti da un processo completamente automatizzato, ad eccezione in cui ci sia il consenso esplicito da parte dell'utente o nei casi autorizzati dalle leggi dell'Unione e degli Stati Membri.

In ogni caso (anche nei casi eccezionali), è previsto comunque il diritto da parte dell'interessato di richiedere l'intervento umano e di contestare la decisione.

Infine nel paragrafo 4 viene proibita la profilazione derivata dall'impiego di particolari categorie di dati personali. Anche in questo caso vengono poste delle eccezioni: tale pratica è

concessa qualora siano presenti adeguate forme di tutela della privacy e della libertà dell'individuo. [13]

Infine, gli articoli 13-15 [14] specificano il diritto ad accedere alle informazioni raccolte su di essi, viene espresso nell'art 14 [15] il diritto di richiedere (nel caso della profilazione), una copia delle informazioni raccolte sul soggetto.

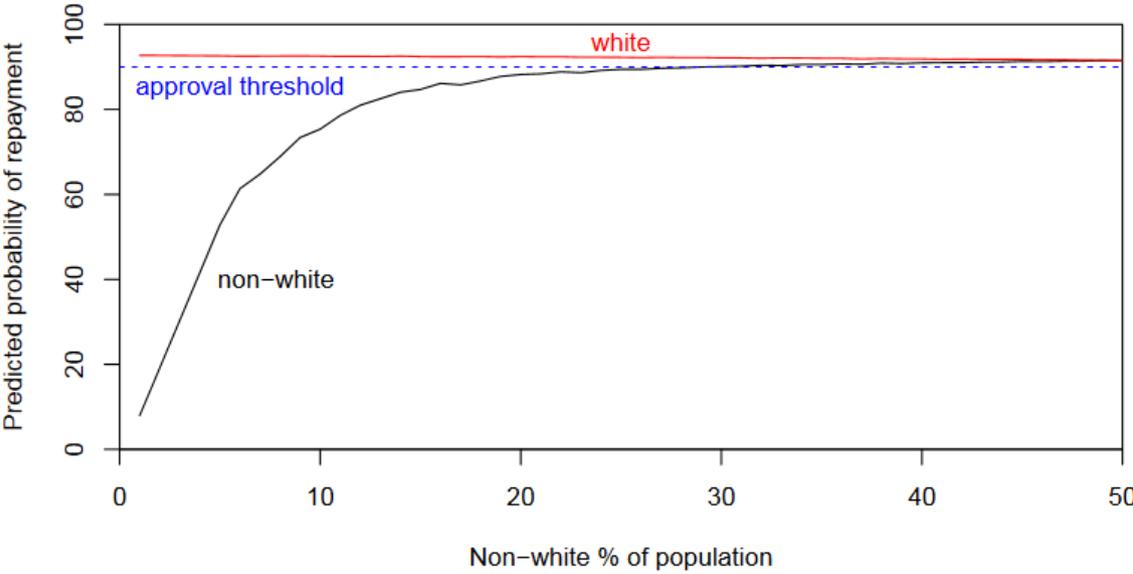
La profilazione secondo categorie di dati personali risulta in aggiunta spesso discriminatoria in quanto tali modelli collezionano i dati secondo le categorie sociali, le quali spesso contengono ineguaglianze o discriminazioni. I modelli nutriti con tali dati spesso riflettono nei risultati tali ineguaglianze.

Proseguendo, nel paragrafo 71 del preambolo del GDPR [16] viene imposta la sorveglianza dei dati e l'utilizzo di misure adeguate alla prevenzione di tali discriminazioni. L'articolo non è così chiaro, ciò lascia spazio a diverse interpretazioni: secondo un'interpretazione "minimalista" l'articolo si applica qualora l'algoritmo utilizzi direttamente dei dati personali; secondo invece l'interpretazione "massimalista" è necessario estendere tali misure anche alle correlazioni che potrebbero essere indirettamente collegate a dei dati personali. Pensiamo ad un algoritmo nutrito con dati geografici, di un'area contenente soggetti con un reddito basso e appartenenti ad una minoranza razziale. Facilmente tale algoritmo riprodurrà tali categorie pur in maniera indiretta.

La seconda interpretazione potrebbe risultare infatti più adeguata, data appunto la capacità di alcuni algoritmi di estrapolare le informazioni partendo da un numero limitato di dati. Come rivelano alcuni consulenti finanziari di Deloitte, [17] alcuni modelli sono in grado partendo dall'analisi di dati come la cronologia degli acquisti, di predire lo status assicurativo degli utenti con precisione pari a quella di un certificato medico. Di fatto, quindi, la capacità di estrapolare delle correlazioni significative anche da dati non direttamente collegati con il risultato richiesto, pone la necessità di impedire l'acquisizione di dati non considerati sensibili. Inoltre, come dimostra un esempio illustrato da Goodman e Flaxman (2017) [18], la scarsa rappresentazione di una categoria può falsare il risultato: nell'esempio viene simulato un algoritmo per il calcolo della probabilità di restituzione di un mutuo. Nell'esperimento vengono create due categorie fittizie di richiedenti: "bianchi" e "non bianchi", tutti gli

individui hanno la probabilità del 95% di ripagare il mutuo indipendentemente dall'appartenenza ai due gruppi. L' algoritmo accetta la richiesta dei richiedenti con probabilità superiori al 90%, il modello inoltre è “risk averse” quindi a parità di condizioni privilegerà le correlazioni sostenute da maggiori dati. I risultati dell'esperimento dimostrano come l'algoritmo concederà il mutuo, in tutti i casi, a tutti i richiedenti “bianchi” mentre per i “non bianchi” (nonostante i dati di partenza identici) l'algoritmo risulta fallace (non concedendo il mutuo) se la popolazione di questi è inferiore al 30% della popolazione totale. Tale esempio dimostra, come l'esperimento riportato nel Capitolo 2, l'esigenza di garantire un'adeguata supervisione ed interpretazione degli algoritmi da parte di un agente umano.

Se il gruppo di “non bianchi” rappresenta una percentuale inferiore al 30% della popolazione totale, l'algoritmo, favorendo le correlazioni più frequenti (in questo caso la maggioranza dei soggetti richiedenti appartiene al gruppo dei “bianchi”), darà un risultato distorto.



### -3.1 Le normative successive al GDPR

Nel 2017 il Parlamento Europeo pubblica una risoluzione sullo stato legale dei robot. Si tratta uno dei primi documenti a livello globale che tratta specificatamente dell'IA. [19]

La risoluzione tratta anche di tematiche più generali, come ad esempio del suo impatto sul mercato del lavoro, o la necessità di introdurre standard di sicurezza e affidabilità. [20]

Inoltre viene espressa la raccomandazione di rispettare le necessarie precauzioni nello sviluppo di nuove tecnologie, oltre a evidenziare il bisogno di pubblicare una normativa compatibile con i valori stabiliti nell'Art 2 del Trattato sull'UE (dignità umana, eguaglianza, giustizia, ecc.). [21]

Più di 200 esperti hanno risposto all'iniziativa del Parlamento Europea tramite una lettera alla CE, sottolineando la mancanza di senso pratico nel dare uno status legale ai robot.

Gli esperti sostengono che le attuali capacità dei robot sono decisamente inferiori e quindi incompatibili con il concetto di personalità legale. [22]

Nonostante ciò la risoluzione evidenzia la volontà da parte dell'UE di sottoporre l'IA ad una regolamentazione che ne possa contenere i rischi, una regolamentazione con un approccio tipicamente Europeo: che combini una logica di libero mercato con i limitata da un forte intervento pubblico. [23]

A seguire, la comunicazione della Commissione Europea del 2018 (la strategia europea in risposta alla feroce competizione globale), dichiara tre obiettivi [24]:

- 1) Alimentare la crescita di investimenti pubblici e privati;
- 2) Anticipare i cambiamenti soci-economici incombenti (lavoro, educazione digitale, welfare adeguato);
- 3) Assicurare una regolamentazione adeguata nel rispetto dei valori europei.

A tale scopo viene proposto nel 2019 il piano IA “Made in Europe” con l'obiettivo di avviare una crescita dell'IA nel rispetto dei valori etici dell'UE. [25]

Il documento sottolinea, in risposta alle iniziative legislative sull'IA già presenti in Francia, Germania e Finlandia, la necessità di creare una strategia comune per massimizzare l'impatto degli investimenti, incoraggiare la cooperazione ed evitare la frammentazione sia del mercato che delle normative in materia.

In particolare viene posta l'attenzione sull'obiettivo di creare un database comune, il che è cruciale per lo sviluppo di un IA competitiva, nel rispetto del GDPR.

Inoltre viene sottolineata la capacità di attrarre gli esperti in materia, ben 240.000 europei infatti lavorano nella Silicon Valley [26], è quindi importante sviluppare delle misure in grado di trattenere i talenti emergenti.

Data la prospettiva globale della strategia, sono stilati 3 obiettivi in materia di sicurezza [27]:

- 1) Impiegare IA nella sicurezza;
- 2) Assicurare IA dagli attacchi esterni;
- 3) Evitare usi illeciti o dannosi dell'IA.

Successivamente viene pubblicato il documento sulle linee guida etiche redatto da un gruppo di esperti in materia di IA nominato dalla Commissione Europea. (2018) HLAIEG (High Level Artificial Intelligence Expert Group)

Il testo ha come scopo definire più precisamente le linee guida etiche menzionate nei documenti precedenti. [28]

Emergono in particolare 3 valori fondamentali [29]:

- 1) Legalità: l'impiego dell'IA dev'essere compatibile con le leggi e i regolamenti esistenti;
- 2) Rispetto dell'etica: rispetto dei valori fondamentali dell'UE;
- 3) Sicurezza e Affidabilità: L'IA non deve arrecare danni a persone o cose, ed essere affidabile dal punto di vista tecnico e sociale.

Son inoltre fissati 7 requisiti per assicurare l'affidabilità dell'IA [30], tra cui: la sorvegliabilità da parte degli operatori umani, il rispetto della privacy, trasparenza, non discriminazione.

La dichiarazione ha ricevuto critiche simili rispetto ai precedenti documenti, in particolare uno dei redattori del testo, Thomas Metzinger, ha espresso le sue preoccupazioni riguardo all'ingerenza degli interessi economici nella redazione del testo [31]. Nonostante egli ammetta i passi avanti fatti con la stesura delle linee guida etiche, critica fortemente la mancanza di una normativa più specifica in aree sensibili e conflittuali come ad esempio le armi automatiche o i sistemi di profilazione. Metzinger definisce la parte in questione “*deliberatamente vaga*” . Egli denuncia la sostituzione, durante la stesura, delle parti dedicate ai temi sopra citati con i termini più generali di “*critical concerns*”. Secondo Metzinger gli interessi economici stanno cercando di guadagnare tempo nei confronti di una regolamentazione che impedirebbe vari abusi.

Al documento sulle linee guida etiche è seguito la proposta da parte della Commissione Europea di un atto unico sull' IA, [32] che potrebbe entrare in vigore a partire dal 2024. Tale atto è la prima proposta avente concreto valore legale, i documenti precedenti, definiti di “soft law” [33] (raccomandazioni, linee guida e il libretto bianco); si limitavano infatti ad esprimere opinioni o raccomandazioni. La proposta di legge dell'aprile 2021 sarebbe quindi il primo atto legislativo esistente a livello globale.

Il documento riprende la logica delle leggi europei in materia di sicurezza, riprendendo la struttura del regolamento sui prodotti del 2008. [34]

Come il GDPR la normativa, pur riferendosi ai fornitori europei, si applicherà anche nei confronti di quelli con sede in stati terzi che vorranno immettere nel mercato nuovi prodotti. [35]

La proposta introduce una classificazione dell' IA secondo 4 criteri di rischio, ciascuna categoria prevede delle condizioni (più o meno stringenti in base alla categoria di rischio) da soddisfare per impiegare legalmente l'IA. [36]

Le categorie, partendo dall'alto, sono le seguenti:[37]

1) “Rischio inaccettabile” ovvero le attività vietate, in quanto considerate dannose o pericolose per la sicurezza della persone e il rispetto dei diritti fondamentali. Tra queste: l'impiego di tecniche manipolative con lo scopo influenzare il comportamento degli utenti, i sistemi di

social scoring o l'identificazione biometrica in tempo reale ed in luoghi pubblici per scopi di pubblica sicurezza e prevenzione dei crimini, ad eccezione dei casi in cui questa sia autorizzata per importanti ragioni di sicurezza dalle autorità degli Stati membri.

2) “Sistemi IA ad alto rischio” come l'identificazione biometrica e la profilazione di persone fisiche ad alto rischio (utilizzati per la sorveglianza), la gestione di operazioni in infrastrutture sensibili come le infrastrutture idriche, elettriche, rete stradale ecc; nell'istruzione, nel mercato del lavoro, con particolare attenzione verso il reclutamento del personale (potenzialmente discriminatorio). Nell'accesso ai servizi pubblici essenziali, nella gestione di sicurezza pubblica e di pubblica sorveglianza, oltre al controllo dell'immigrazione e nella gestione delle frontiere, nell'amministrazione della giustizia e dei servizi elettorali.

Le attività sopra elencate devono soddisfare svariati requisiti a partire dall'adozione di misure adeguate al contenimento dei rischi, garantendo la necessaria trasparenza e comprensibilità dell'algoritmo da parte degli utenti, dimostrando di poter operare con sufficiente affidabilità e robustezza, assicurando il rispetto delle linee guida sopra elencate.

Sono menzionate inoltre ulteriori obblighi per i fornitori non europei tra cui: il superamento di un giudizio di conformità rispetto alla destinazione, la sottoscrizione ad un registro europeo dedicato all'IA e la nomina di un rappresentante in grado di garantire e dimostrare la compatibilità coi criteri annunciati.

3) Sistemi a rischio limitato: come chatbot, sistemi di profilazione biometrica a basso rischio (a scopo di categorizzazione), sistemi “deepfake” (addetti alla pubblicazione/manipolazione di testi, file audio o immagini).

Tali sistemi sono soggetti esclusivamente ad obblighi di trasparenza previsti nel Titolo V.

4) Sistemi a basso o minimo rischio: tali sistemi non sono sottoposti a nessuna obbligazione, viene raccomandata esclusivamente la stipulazione di un codice di condotta facoltativo per incoraggiare i fornitori ad auto conformarsi alle norme previste per le altre categorie.

Il documento esclude dalla normativa l'IA impiegata in campo militare e le tecnologie utilizzate dalle autorità pubbliche nello svolgimento delle attività di pubblica sicurezza o cooperazione giudiziaria. [38]

Si ripete quindi quanto accaduto con la pubblicazione dei documenti precedenti.

L'Unione Europea al momento è l'unica istituzione ad aver dimostrato serie intenzioni nel produrre uno specifico regolamento sull'IA. In confronto USA e UK [39] si sono finora impegnati nel definire strategie sullo sviluppo dell'IA, ignorando però la possibilità di pubblicare un codice dedicato come l'atto unico.

Diversi studiosi denunciano la pericolosità delle ingerenze economiche nel processo normativo, e la difficoltà di sviluppare delle tecnologie competitive a livello globale che non compromettano i principi stabiliti. [40]

Inoltre si segnala la mancanza di una strategia per l'applicazione, a livello nazionale e locale delle linee guida elencate, che tenga inoltre conto delle differenze di sviluppo economico e sociale tra i vari stati dell'Unione. [41] In particolare tenendo conto del recente sviluppo di strategie sull'IA in vari paesi, è necessario uno sforzo maggiore per garantire l'uniformità della normativa e del mercato. [42] Tale sforzo dovrebbe altresì essere supportato da una adeguata metodologia con maggiore attenzione verso le applicazioni attuali. [43]

E' necessaria inoltre una delimitazione più precisa delle competenze dell'IA con riferimento soprattutto alla sorvegliabilità da parte degli agenti umani.[44] In riferimento a quanto già detto sulla nebulosità che circonda l'elaborazione di alcuni risultati, si potrebbe ad esempio imporre la supervisione e l'approvazione da parte di esperti umani, sui risultati elaborati da un algoritmo. A livello istituzionale sarebbe auspicabile la creazione di organismo (simile al Garante delle Privacy) in grado di vigilare sull'operato degli algoritmi e di emettere sanzioni. Oltre a ciò la maggior parte delle misure previste si basa largamente sull'autoregolamentazione da parte dei fornitori dei servizi (ai veda cat. Low risk, pagina precedente) e non viene per ora infatti menzionato un meccanismo di arbitraggio tecnicamente valido e adeguato a tutela dei singoli utenti.

Con riferimento al documento sulle linee guida, è da segnalare l'adozione di una definizione di IA assai generale, senza un adeguato approfondimento delle differenze sostanziali tra le

varie discipline e tecnologie. Ciò impedisce di concentrarsi su dettagli specifici e contestuali [45], ostacolando quindi l'implementazione di misure più mirate e concrete.

Rimane poi ambigua la relazione tra la volontà di sviluppare tecnologie competitive a livello globale e il rispetto e la tutela della privacy, in particolare riguardo all' approvvigionamento dei dati personali: nei testi non vengono fornite spiegazioni sufficienti e precise su come si possano compilare enormi database nel rispetto dei principi annunciati.

Riguardo alla sicurezza e all'inviolabilità degli algoritmi, non vengono menzionate misure di sicurezza obbligatorie e dettagliate su questo aspetto, con riferimento particolare alla protezione nei confronti di potenziali attacchi informatici.

Infine è poco considerato l'aspetto ambientale, come specificato nel capitolo 1.6, l'IA potrebbe risultare uno strumento particolarmente utile ed allo stesso tempo nocivo per la tutela dell'ambiente [46].

### - 3.2 European Data Strategy

L'UE ha pianificato una strategia comune in materia di dati, con obiettivo di creare uno spazio comune europeo in grado di garantire un'alta qualità di dati sempre nel rispetto dei limiti imposti dal GDPR, riducendo inoltre le emissioni inquinanti secondo gli standard del Green Deal. [1]

Non è la prima volta nella storia Europea che si assiste al tentativo di uniformare un determinato settore economico, sin dagli albori dell'UE è infatti presente questo tipo di sforzo. [2]

La creazione di una normativa comune può consentire alle imprese europee di fornire servizi competitivi nel rispetto dei diritti personali degli utenti, limitando inoltre i costi ambientali. Elaborando inoltre una risposta valida nei confronti dell'oligopolio delle aziende cinesi e della Silicon Valley. [3] Tale strategia ha l'obiettivo di migliorare la circolazione dei dati all'interno dell'Unione in modo da sfruttare il valore di questi per finalità pubbliche. Ad esempio ottenendo un miglioramento dei servizi da parte degli enti pubblici, oppure favorendo la

produttività delle piccole medie imprese. [4] Ciò sarebbe raggiungibile determinando le strutture e i soggetti (e le modalità oltre alle finalità) in grado di beneficiare all'accesso dei dati.

In particolare la strategia si pone 4 obiettivi [5]: *The strategy builds on four pillars: (i) establishing a cross-sectoral governance framework for data access and use, most notably by regulating data-sharing,*

*(ii) strengthening Europe's data spaces and cloud infrastructure, for instance by co-investing approximately €2 billion (of a combined investment of about €4-6 billion) in infrastructure, data-sharing tools, architecture and governance mechanisms,*

*(iii) empowering individuals to control their data, as well as investing in skills and capacity-building, and*

*(iv) promoting the development of at least nine common European data spaces in strategic sectors and domains of public interest, such as manufacturing, Green Deal, health and finance.*

1) Data Government Act: Proposto nel 2020, è il primo pilastro della strategia europea che si propone di rendere più accessibile l'enorme potenziale dei dati, rafforzando i diritti di imprese e privati circa il possesso dei dati provenienti dall'uso personale. Il testo mira infatti a stabilire delle norme che possano rafforzare la posizione economica delle imprese e degli utenti europei nel mercato dei dati. [6] Rispetto al GDPR in cui la materia è trattata dal punto di vista della privacy, il DGA affronta il tema dal punto di vista economico-sociale considerando i dati come bene di scambio.

L'obiettivo è di garantire maggiore controllo da parte degli stessi utenti sui propri dati, oltre a permettere alle imprese di piccole, medie o grandi dimensioni di accedere o condividere dati senza grandi barriere di accesso. [7]

In aggiunta, viene istituita la figura del "Data Altruist", [8] ovvero viene consentita la possibilità da parte di un utente di "donare" i propri dati a dei soggetti qualificati per determinate finalità.

Un esempio potrebbe essere un soggetto affetto da una malattia cronica che condivide i propri dati ad un' associazione no-profit con lo scopo di aiutare la ricerca medica in materia.

Per soggetti qualificati, [9] si intendono dei soggetti autorizzati in grado di dimostrare sufficienti requisiti di trasparenza, oltre ad adeguate misure di sicurezza per la protezione dei dati detenuti.

Le operazioni citate devono però garantire i diritti di privacy degli utenti, per tale ragioni è reso necessario stabilire adeguate misure tecniche per garantire l'anonimato. In caso di circolazione o utilizzo da parte di più soggetti dei medesimi dati, è opportuno garantire inoltre la segretezza commerciale imposta dal GDPR. [10]

Viene prevista per giunta la regolamentazione della figura di un intermediario nello scambio di dati [11], ovvero un soggetto autorizzato a supervisionare la diffusione dei dati. Secondo il testo sono previste inoltre specifiche e più severe misure per quanto riguarda il data sharing rispetto alle altre attività di analisi dati. Viene infatti imposta la sorveglianza pubblica (per il data sharing), oltre all'iscrizione in un apposito registro.

L'atto permette inoltre la diffusione di dati detenuti da enti pubblici nei confronti di imprese, amministrazioni pubbliche, e verso istituti impegnati nella ricerca accademica. [12] Tali dati sono spesso caratterizzati dalla presenza di dati sensibili su individui o imprese [13]. Come descritto precedentemente, rimane cruciale garantire la relativa privacy attraverso specifiche misure tecniche, bilanciando la possibilità di sbloccare il potenziale di tali dati sempre nel rispetto della privacy dei soggetti interessati.

2) Data act: Pubblicato nel Febbraio 2022, con lo scopo di colmare la mancanza di chiarezza riguardo all'accesso e utilizzo dei dati stabiliti nelle precedenti normative. In particolare è rivolta particolare attenzione verso la posizione delle piccole medie imprese, le quali faticano a beneficiare di tali tecnologie, per via dei costi e della debole posizione contrattuale nei confronti dei fornitori di tali servizi. In particolare il testo stabilisce i soggetti e le modalità autorizzati a creare valore dai dati. [14]

La normativa risponde alla necessità proveniente dalla crescente diffusione dei dispositivi intelligenti, i quali spesso non determinano in maniera chiara chi siano i “beneficiari” dei dati, ovvero coloro che possono sfruttarli tramite la raccolta e l'analisi. [15]

Il testo intende estendere i diritti degli utenti e delle imprese nei confronti dell'alienabilità dei dati, in maniera tale da incentivare la circolazione di questi. [16]

Ad esempio il proprietario di auto intelligente potrà decidere se donare i dati generati dall'auto ad una compagnia assicurativa oppure all'ente pubblico responsabile della viabilità, in modo da poter migliorare il funzionamento della rete stradale. [17]

Tale circolazione di dati favorirebbe le piccole/medie imprese, le quali potrebbero più facilmente avere accesso ai dati contrastando la concentrazione di ricchezza che caratterizza il mercato dei dati. Un maggiore accesso a questi può garantire inoltre il miglioramento di diversi servizi, oltre alla possibilità di garantire una gestione più efficiente delle risorse, con effetti benefici dal punto di vista climatico. [19] Tuttavia, come è stato espresso nei capitoli precedenti l'impatto delle tecnologie IA è ancora difficilmente quantificabile e prevedibile. Sempre riguardo alle PMI (Piccole Medie Imprese) il testo stabilisce l'illegalità delle clausole imposte unilateralmente da parte dai grandi fornitori, ovvero di condizioni che possano pregiudicare la stipula di contratti equi [20]. Allo stesso tempo è annunciata la possibilità di stabilire in maniera libera al di fuori delle clausole "inique", in modo da poter agevolare la stipula dei contratti in considerazione delle diverse condizioni presenti all'interno del mercato europeo.

Viene incluso, in aggiunta, il diritto da parte degli enti pubblici, di poter accedere a dati detenuti da parte di soggetti privati, in determinati casi. Ad esempio qualora sia necessario far prevalere un interesse pubblico superiore o far fronte ad una pubblica emergenza. Viene previsto come nel caso dell'istituto giuridico dell'espropriazione una giusta ricompensa al soggetto privato. [21]

Data l'importanza dei servizi di "data processing", viene ammessa la possibilità di scambiare dati tra soggetti diversi senza incorrere in costi aggiuntivi. E' prevista inoltre l'istituzione di misure standardizzate per lo scambio di dati e di accesso ai servizi cloud. [22]

A tutela dei dati detenuti nei servizi cloud vengono imposte delle misure obbligatorie connesse alla detenzione di dati. [23]

Inoltre i titolari di piccole medie imprese (PMI) saranno protetti dal regolamento, al fine di impedire la stipulazione di contratti che ostacolino l'accesso ai dati.

Ad esempio un imprenditore agricolo che acquista un software per l'ottimizzazione della gestione dei terreni avrà il diritto ad ottenere le informazioni rilevanti per la sua attività. [24]

Riguardo ai diritti di terze parti rispetto ai dati generati dai proprietari degli oggetti intelligenti, viene imposto il divieto da parte di questi di utilizzare tali dati in qualsiasi maniera che danneggi o possa danneggiare il titolare dell'oggetto o del servizio. [25]

Il Data Act inoltre riprende le regole imposte dal GDPR riguardo al trattamento di dati sensibili. Rispetto a quest'ultima normativa, la quale limitava la portabilità dei dati da parte dell'utente, ovvero la possibilità di divulgare i propri dati a terzi. Nel GDPR, la portabilità dei dati era consentita solo a determinate condizioni legali, e limitata ai soli dati personali. Il Data Act ha annunciato quindi l'estensione del diritto di portabilità degli utenti anche ai dati non sensibili, ed in generale a condizioni meno severe rispetto al GDPR. [26]

Infine è prevista l'istituzione dello spazio comune europeo in materia. [27] Al fine di offrire servizi più competitivi ed economici, sarà quindi agevolata una più facile circolazione dei dati. E' annunciata inoltre la creazione di 10 spazi comuni dedicati a settori strategici come agricoltura, sanità, energia, ecc. in accordo con gli obiettivi posti dal Green Deal. [28]

La normativa prevede dunque un'attenuazione delle condizioni relative alla circolazione dei dati, il testo si pone come obiettivo principale l'eliminazione delle barriere al pieno dispiegamento del potenziale economico di questi.

Ciò sarebbe consentito ad esempio dalla maggiore "portabilità" conferita ad utenti e imprese, è opportuno però sottolineare a proposito la relazione tra la responsabilità conferita ad un soggetto di disporre dei dati generati e l'effettiva educazione digitale dell'utente medio. Tale aspetto si può considerare un limite della normativa; è auspicabile quindi l'istituzione di misure che educino all'uso dei dispositivi digitali.

Allo stesso modo, la normativa, considerando dal punto di vista economico la diffusione dei dati, riconosce per lo meno maggior controllo e maggiori diritti da parte degli utenti rispetto alle informazioni da loro generate.

La riduzione dell'incertezza relativa ai diritti circa ai dati prodotti dalle tecnologie IoT [29] (Internet of Things) potrebbe ostacolare l'oligopolio di tali informazioni descritto da Zuboff, (capitolo 1.5) assicurando maggiore chiarezza, unita al riconoscimento di maggiori diritti degli utenti potrebbe quindi deviare la ricchezza dai dati dagli interessi privati verso un uso pubblico.

In particolare riconoscendo la situazione di inferiorità dei soggetti meno tutelati come le PMI viene comunque definito il diritto ad una maggiore diffusione della ricchezza derivante dai dati rispetto all'iniqua concentrazione attuale.

Inoltre è da segnalare positivamente la prevalenza in determinate casistiche dell' interesse pubblico rispetto a quello privato, in maniera simile all'istituto giuridico dell'espropriazione. Più in generale è presente il tentativo di incentivare una maggiore diffusione di tale potenziale economico, riconoscendo maggiore importanza all'uso pubblico di tali tecnologie quale la gestione delle risorse, il monitoraggio del cambiamento climatico, o il miglioramento delle infrastrutture.

#### 4 – Conclusioni

Attualmente l'IA è largamente impiegata in un numero crescente di mansioni e settori, nel prossimo futuro ci si aspetta inoltre una maggiore diffusione di tali tecnologie. (capitolo 1.2)

l'IA ha un peso fondamentale in termini economici: infatti occupa e occuperà una fetta sempre più consistente dell'economia mondiale.

L'importanza economica che riveste, rende lo sviluppo dell'IA un terreno di contesa tra le potenze globali (capitolo 1.3): come abbiamo visto la ricerca impegna in maniera importante vari paesi come USA e Cina che mirano a stabilire la propria leadership a livello globale. In generale è dimostrabile come proprio questa tecnologia contribuisce e contribuirà a stabilire le varie sfere d'influenza globali, specialmente attraverso l'istituzione di vere e proprie colonie digitali che favoriranno i paesi detentori di tali tecnologie.

A livello di politica domestica, (capitolo 1.4) è stata dimostrata col recente scandalo di Cambridge Analitica (2016) la forte influenza proveniente dall'uso delle tecniche di

profilazione in materia elettorale. Inoltre, la diffusione delle piattaforme di comunicazione quali Facebook o Twitter ha smentito le speranze riguardo ad un avanzamento della partecipazione democratica ottenibili tramite tali piattaforme, dimostrandosi al contrario nocive in questo senso. Contribuendo invece a confermare i pregiudizi esistenti piuttosto che contribuire al dialogo tra posizioni diverse.

Le tecnologie IA, come già espresso in precedenza, sono alla base dei servizi forniti da compagnie come Google, Facebook, Amazon, Microsoft ecc. Vari fattori hanno portato alla monopolizzazione di tali tecnologie da parte dei grandi marchi dell'high tech ed alla creazione di un meccanismo economico definito “Economia della Sorveglianza” (capitolo 1.5). Questo è basato sull' estrazione delle informazioni personali degli utenti al fine di elaborare, tramite l'uso delle tecnologie IA, annunci personalizzati o vere e proprie previsioni dei comportamenti degli utenti a fini commerciali.

Oltre alla palese violazione della libertà personale degli utenti di tali servizi, tale monopolio ha impedito o limitato lo sviluppo di tecnologie IA potenzialmente utili (come nel caso dell'algoritmo Realeyes), attraverso l'assorbimento quasi totale delle risorse umane nel settore. Instaurando inoltre una barriera a difesa degli interessi delle compagnie menzionate tramite una aggressiva campagna di finanziamenti diretti ad alcuni personaggi politici di spicco.

Dal punto di vista ambientale, (capitolo 1.6) è importante menzionare la rilevanza della futura gestione dell'IA, in riferimento al cambiamento climatico in corso. Nonostante risulti assai complicato quantificare precisamente le emissioni prodotte dall'IA, questa contribuisce in maniera importante al consumo energetico. Contemporaneamente la si può definire uno strumento fondamentale per la creazione di uno stile di vita sostenibile. Ad esempio risultano assai utili i sistemi di monitoraggio ambientale, inoltre in svariati settori l'IA permette una gestione più efficiente delle risorse. Si può ritenere quindi necessaria l'istituzione di norme precise che tengano conto di questo aspetto.

In aggiunta, come è stato esposto (capitolo 2), molti algoritmi risultano faticosamente decifrabili, ovvero sono, dal punto di vista di un osservatore esterno, vere e proprie scatole, nere.

Lo sviluppo di tali algoritmi sacrifica spesso una necessaria spiegazione del processo che determina i risultati, generando svariati problemi in relazione all'impiego nel mondo reale di tali modelli. Tale problema sottolinea la necessità di comprendere e quindi di tutelarsi da parte dei soggetti interessati, e di determinare eventuali responsabilità; in caso di incidenti. E' inoltre importante garantire la comprensione del processo decisionale degli algoritmi al numero maggiore possibile di utenti. In modo da limitare l'asimmetria di potere tra questi e i fornitori di tali servizi, favorendo inoltre un maggiore controllo da parte degli utenti stessi. Infine, la mancanza di trasparenza rende difficile identificare eventuali violazioni dei diritti personali nei confronti dei soggetti da parte del trattamento, oscurando eventualmente determinati usi illeciti o impropri dei dati.

Strumenti come il modello LIME possono agevolare tali compiti, consentendo in parte il diretto controllo degli individui nei confronti delle tecnologie che li circondano.

A livello internazionale si riscontra finora una flebile risposta legislativa ai problemi menzionati. I paesi dell'UE sono per ora gli unici ad aver dimostrato l'intenzione di produrre una normativa dettagliata riguardo l'impiego dell'IA.

A partire dal 2016 (capitolo 3), l'UE ha pubblicato atti non aventi potere vincolante (Soft Law), limitando ad esprimere raccomandazioni a riguardo ed invitando i vari attori ad un'auto-regolamentazione dei servizi legati all'IA.

Solo nel 2020, è stata annunciata la volontà di regolamentare in maniera vincolante le tecnologie IA, attraverso un regolamento simile alla presente normativa sulla sicurezza dei prodotti. L'atto è ancora in fase di approvazione e dovrebbe entrare in vigore nel 2024.

Questo vincola l'impiego dell'IA al soddisfacimento di determinati requisiti, essi sono stabiliti secondo una classificazione dei rischi derivanti dall'adozione delle varie tecnologie. Ad esempio, i sistemi classificati ad alto rischio, come la profilazione biometrica in tempo reale, richiedono determinati requisiti di trasparenza, nonché il superamento di un giudizio di conformità, e l'iscrizione ad un registro europeo dedicato. Logicamente al diminuire del rischio riconosciuto sono previste misure meno stringenti fino ad arrivare all'assenza di obbligazioni da parte dei fornitori nel caso dei sistemi a "basso rischio".

La normativa, sebbene sia decisamente avanzata nel contesto globale, non è dotata attualmente della necessaria precisione e specificità: sono fissati per ora i principi guida etici oltre alle categorie di rischio, devono però essere implementati degli indicatori specifici riguardo a ciascun tipo di tecnologia. Come espresso nell'Introduzione, la definizione di IA utilizzata dall'UE si riferisce ad una famiglia di tecnologie accomunate da un certo grado di autonomia. Tale definizione quindi comprende strumenti assai diversi: dai sistemi di riconoscimento facciale, alla robotica, fino alle macchine a guida autonoma. Ciò implica la necessità di stabilire norme specifiche per ogni tecnologia. Rimane per ora incompiuto tale passaggio, per altro piuttosto urgente visto il già ampio e diffuso impiego dell'IA in diversi contesti.

Bisogna segnalare comunque, il riconoscimento, da parte della normativa europea, del potenziale economico dei dati, e la definizione di diritti quantomeno più chiari circa la detenzione e l'uso economico dei dati.

Sebbene dal mio punto di vista esista una notevole asimmetria culturale tra i diritti conferiti agli utenti e l'effettiva educazione digitale di questi, bisogna comunque notare nella strategia europea una crescente attenzione verso il riconoscimento degli interessi pubblici in merito. Nonostante ciò la ricchezza dell'IA rimane tutt'ora largamente concentrata e lontana dall'essere pubblica. Come abbiamo visto, il potenziale economico e politico rende l'IA determinante nella definizione degli equilibri di potere geopolitico. Inoltre dal punto di vista della politica interna l'utilizzo dei Social Network risulta fondamentale nel futuro sviluppo della vita democratica, come mostrato nel capitolo 1.4.

Da diversi punti di vista è possibile quindi concludere che l'IA influenza e probabilmente influenzerà sempre più pesante le nostre vite, al punto da poter determinare la sopravvivenza della nostra biosfera.

Il testo ha come obiettivo dimostrare il profondo impatto economico, sociale, politico, di tale tecnologia. E' opportuno inoltre considerare che l'IA è una tecnologia in rapido sviluppo, verso la quale è difficile fare previsioni circa la futura evoluzione. Tra gli esperti in materia si trovano pareri decisamente discordanti: chi come Bostrom o Kurzweil considera prossimo l'avvento della SuperIntelligenza o chi si dimostra scettico a proposito, come Faggin.

La tecnologia infatti è stata in grado di alterare le dinamiche evolutive consentendo all'uomo di dominare il pianeta. Per ora tutto ciò rimane pura speculazione ma non si può allo stesso tempo escludere che l'IA possa un giorno uguagliare e superare la nostra intelligenza, forse decretando la fine dell'umanità oppure consentendoci di superare i limiti naturali tramite l'unione tra uomo e macchina.

## BIBLIOGRAFIA

Introduzione.

1. High-Level Expert Group on Artificial Intelligence , European Commission, A DEFINITION OF AI: MAIN CAPABILITIES AND DISCIPLINES (2018), p 1  
<https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>
2. Walter Bock, The Definition and Recognition of Biological Adaptation (1980), p 221  
[https://www.researchgate.net/publication/31442829\\_The\\_Definition\\_and\\_Recognition\\_of\\_Biological\\_Adaptation/link/00463532ec0de49a98000000/download](https://www.researchgate.net/publication/31442829_The_Definition_and_Recognition_of_Biological_Adaptation/link/00463532ec0de49a98000000/download)
3. Higham, Timothy & Anderson, Christopher. (2014). Function and adaptation of chameleons, p73  
[https://www.researchgate.net/publication/258345857\\_Function\\_and\\_adaptation\\_of\\_chameleons/link/00463528be0636dd8b000000/download](https://www.researchgate.net/publication/258345857_Function_and_adaptation_of_chameleons/link/00463528be0636dd8b000000/download)
4. Margaret Pholip (2001), Paleolithic technology and human evolution, pp 1749-51  
[https://www.academia.edu/2153649/Paleolithic\\_technology\\_and\\_human\\_evolution](https://www.academia.edu/2153649/Paleolithic_technology_and_human_evolution)
5. ibid
6. Dennis M. Sandgathe and Francesco Berna, Fire and the Genus Homo, Current Anthropology Volume 58, p 6  
<https://www.journals.uchicago.edu/doi/epdf/10.1086/691424> -
7. Ray Kurzweil, Singularity is near (2005), p.9
8. Nick Bostrom, 2003, chapter 4.4 , “Badly programmed Superintelligence”  
<https://ora.ox.ac.uk/objects/uuid:827452c3-fcba-41b8-86b0-407293e6617c>,
9. Ray Kurzweil, Singularity is near (2005), p.56
10. ibi, p.51-56
11. ibi, p.9
12. ibi, p. 149,150
13. Federico Faggin, A.I Challenge, Chiara Sottocorona, 2019, pp 31-37
14. Federico Faggin, A.I Challenge, Chiara Sottocorona, 2019, pp 31-37
15. Ray Kurzweil, Singularity is near (2005), p.10

### Capitolo Primo

1.1 Storia dell'IA.

1. Barrios Tao, Hernando & Pérez, Vianney & Guerra Post Ph.D., Yolanda. (2019). 2019 72(12 ) 30  
ARTIFICIAL INTELLIGENCE AND EDUCATION Challenges and disadvantages for the teacher 1. Arctic  
medical research. 72. 30-51. p 32

[https://www.researchgate.net/profile/Vianney-Perez/publication/338236746\\_2019\\_7212\\_30\\_ARTIFICIAL\\_INTELLIGENCE\\_AND\\_EDUCATION\\_Challenges\\_and\\_disadvantages\\_for\\_the\\_teacher\\_1/links/6023e1cf458515893996fcb7/2019-7212-30-ARTIFICIAL-INTELLIGENCE-AND-EDUCATION-Challenges-and-disadvantages-for-the-teacher-1.pdf](https://www.researchgate.net/profile/Vianney-Perez/publication/338236746_2019_7212_30_ARTIFICIAL_INTELLIGENCE_AND_EDUCATION_Challenges_and_disadvantages_for_the_teacher_1/links/6023e1cf458515893996fcb7/2019-7212-30-ARTIFICIAL-INTELLIGENCE-AND-EDUCATION-Challenges-and-disadvantages-for-the-teacher-1.pdf) ,

2. Buchanan, B. G. (2005). A (Very) Brief History of Artificial Intelligence. *AI Magazine*, 26(4), p 53.  
<https://doi.org/10.1609/aimag.v26i4.1848>, p 1 <https://ojs.aaai.org/index.php/aimagazine/article/view/1848>,
3. *ibid.*
4. Bruce J. MacLennan, A Summary of the History of AI Before Computers, (2007), p 6  
<https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.75.5118&rep=rep1&type=pdf>,
5. *ivi*, p.8
6. Mijwil, Maad. (2015). History of Artificial Intelligence. 3. 1-8. 10.13140/RG.2.2.16418.15046. p. 2  
[https://www.researchgate.net/publication/322234922\\_History\\_of\\_Artificial\\_Intelligence](https://www.researchgate.net/publication/322234922_History_of_Artificial_Intelligence),
7. *ivi*, p 1,2
8. Dick, S. (2019). Artificial Intelligence. *Harvard Data Science Review*, 1(1).  
<https://doi.org/10.1162/99608f92.92fe150c> <https://hdsr.duquduq.org/pub/0aytgrau/release/1>
9. *Russell, Stuart J.; Norvig, Peter (2003), Artificial Intelligence: A Modern Approach (2nd ed.), Upper Saddle River, New Jersey: Prentice Hall, ISBN 0-13-790395-2*, p. 17.
10. Mijwil, Maad. (2015). History of Artificial Intelligence. 3. 1-8. 10.13140/RG.2.2.16418.15046. p.5  
[https://www.researchgate.net/publication/322234922\\_History\\_of\\_Artificial\\_Intelligence](https://www.researchgate.net/publication/322234922_History_of_Artificial_Intelligence),
11. *ibid.*
12. *ivi*, p 5 e ss.
13. *ibid*
14. Li Deng and Dong Yu (2014), "Deep Learning: Methods and Applications", Foundations and Trends® in Signal Processing: Vol. 7: No. 3–4, pp 197-387. <http://dx.doi.org/10.1561/2000000003>, p 5  
<https://www.nowpublishers.com/article/Details/SIG-039>

## 1.2 Attuali impieghi dell'IA.

1. Meredith Broussard, Artificial Unitelligence, (2018), p 15.
2. European Parliamentary Research Service, Author: Marcin Szczepański, Economic impact of Artificial intelligence (AI) 2019, p 3  
[https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/637967/EPRS\\_BRI\(2019\)637967\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/637967/EPRS_BRI(2019)637967_EN.pdf),
3. *ibid*, p.6
4. *ibid*,
5. *ivi*, p.7

6. Shoshana Zuboff, *Surveillance Capitalism*, 2016, p.63 e ss.
7. *ivi.*, p 70
8. Self-driving cars in the EU: from science fiction to reality, 2019  
<https://www.europarl.europa.eu/news/en/headlines/economy/20190110STO23102/self-driving-cars-in-the-eu-from-science-fiction-to-reality>
9. ARTIFICIAL INTELLIGENCE AND LIFE IN 2030 ONE HUNDRED YEAR STUDY ON ARTIFICIAL INTELLIGENCE | REPORT OF THE 2015 STUDY PANEL, p 24 <https://apo.org.au/sites/default/files/resource-files/2016-09/apo-nid210721.pdf>,
10. *ivi.*, p 25 e ss
11. *ivi.*, p 36 e ss

### 1.3 L'IA nel contesto geopolitico attuale

1. Radina Gigova, Who Vladimir Putin thinks will rule the world, 2017  
<https://edition.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html>
2. Shoshana Zuboff, *Surveillance Capitalism*, 2016, p.63 e ss.
3. Nicolas Miaillhe, «The geopolitics of artificial intelligence: The return of empires?», *Politique étrangère* 2018/3 (Autumn Issue) , p. 7 , <https://www.cairn-int.info/journal-politique-etrangere-2018-3-page-105.html>
4. *ibid.*
5. *ibid.*
6. Arnab Kumar, Punit Shukla, Aalekh Sharan and Tanay Mahindru of NITI Aayog, Discussion Paper National Strategy for Artificial Intelligence, 2018  
[https://www.niti.gov.in/writereaddata/files/document\\_publication/NationalStrategy-for-AI-Discussion-Paper.pdf](https://www.niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf)
7. Tim Dutton, An Overview of National AI Strategies, 2018  
<https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd>, Poland
8. Bloomberg News, “AI Will Add \$15.7 Trillion to the Global Economy,” *Bloomberg News*, June 28, 2017, accessed September 20, 2018, <https://www.bloomberg.com/news/articles/2017-06-28/ai-seen-adding-15-7-trillion-as-game-changer-for-global-economy>.
9. Louise Lucas, “US-China Tech Wars Threaten Global Sector Disruption,” *Financial Times*, May 7, 2018, accessed September 20, 2018, <https://www.ft.com/content/659fb304-4a00-11e8-8ee8-cae73aab7ccb>.
10. Rani Molla, “Tech Companies Spend More on R&D Than Any Other Companies in the U.S.,” *Recode*, September 1, 2017, accessed September 20, 2018, <https://www.recode.net/2017/9/1/16236506/tech-amazon-apple-gdp-spending-productivity>.

11. Jeffrey Ding, “Deciphering China’s AI Dream,” Future of Humanity Institute, University of Oxford, March 2018, accessed September 20, 2018,. p 29  
[https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering\\_Chinas\\_AI-Dream.pdf](https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf),
12. Jingwang Li, “2017 China-US AI Venture Capital State and Trends Research Report,” IT Juzi and Tencent Institute, 2017.
13. Mckinsey Globan Ins, DIGITIZATION, AI, AND THE FUTURE OF WORK: IMPERATIVES FOR EUROPE, 2017, p. 4 <https://www.mckinsey.com/featured-insights/europe/ten-imperatives-for-europe-in-the-age-of-ai-and-automation>
14. European Parliamentary Research Service, Author: Marcin Szczepański, Economic impact of Artificial intelligence (AI) 2019, p 3
15. Nikolai Markotkin and Elena Chernenko, “Developing Artificial Intelligence in Russia: Objectives and Reality,” Aug. 5, 2020, <https://carnegie.ru/commentary/82422>; “Artificial Intelligence Startups in Russia,” Tracxn, April 16, 2020, <https://tracxn.com/explore/Artificial-Intelligence-Startups-in-Russia>; “Artificial Intelligence Startups in United States,” Tracxn, April 16, 2020, <https://tracxn.com/explore/ArtificialIntelligence-Startups-in-United-States>; “Artificial Intelligence Startups in China,” Tracxn, April 16, 2020, <https://tracxn.com/explore/Artificial-Intelligence-Startups-in-China>.
16. Keith Dear, “Will Russia Rule the World Through AI?,” RUSI Journal, Nov. 29, 2019, <https://doi.org/10.1080/03071847.2019.1694227>.
17. Alina Polyakova, “Weapons of the weak: Russia and AI-driven asymmetric warfare,” Brookings Institution, Nov. 15, 2018, <https://www.brookings.edu/research/weapons-of-theweak-russia-and-ai-driven-asymmetric-warfare/>
18. S. Petrella, Chris Miller, and Benjamin Cooper, Russia’s Artificial Intelligence Strategy: The Role of State-Owned Firms November, 2020 , p. 78
19. *ivi*, p 82, 91, 97.
20. *ivi*, p 80
21. *ivi*, p 84
22. Nicolas Miailhe, «The geopolitics of artificial intelligence: The return of empires?», *Politique étrangère* 2018/3 (Autumn Issue) , p. 11 , <https://www.cairn-int.info/journal-politique-etrangere-2018-3-page-105.html>
23. *ibid*.
24. *ibid*, <https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/>
25. Nicolas Miailhe, «The geopolitics of artificial intelligence: The return of empires?», *Politique étrangère* 2018/3 (Autumn Issue) , p. 11 , <https://www.cairn-int.info/journal-politique-etrangere-2018-3-page-105.html>
26. [https://www.lemonde.fr/afrique/article/2018/06/17/intelligence-artificielle-en-afrique-le-risque-de-captation-de-valeur-existe-decrypte-cedric-villani\\_5316644\\_3212.html](https://www.lemonde.fr/afrique/article/2018/06/17/intelligence-artificielle-en-afrique-le-risque-de-captation-de-valeur-existe-decrypte-cedric-villani_5316644_3212.html)

#### 1.4 L'IA nella politica interna.

1. Mijwil, Maad. (2015). History of Artificial Intelligence. 3. 1-8. 10.13140/RG.2.2.16418.15046. p.1-3  
[https://www.researchgate.net/publication/322234922\\_History\\_of\\_Artificial\\_Intelligence](https://www.researchgate.net/publication/322234922_History_of_Artificial_Intelligence),
2. Buchanan, B. G. (2005). A (Very) Brief History of Artificial Intelligence. *AI Magazine*, 26(4), p 54  
<https://doi.org/10.1609/aimag.v26i4.1848>, <https://ojs.aaai.org/index.php/aimagazine/article/view/1848>,
3. Shoshana Zuboff, *Surveillance Capitalism*, 2016, pp.112-115
4. Shoshana Zuboff, *Surveillance Capitalism*, 2016, p.117
5. *ibid*, 122-124
6. *ibid*, 278-281
7. *ibid*, 279-281
8. *ibid*, 273
9. Paul Ekman (1992) An argument for basic emotions, *Cognition and Emotion*, 6:3-4, 169-200, DOI:  
[10.1080/02699939208411068](https://doi.org/10.1080/02699939208411068), R Pickard, *Affective Computing*, 1997, Chapter 3
10. "The Repertoire of Nonverbal Behavior: Categories, Origins, Usage and Coding," *Semiotica* 1, no. 1 (1969): 49–98; Paul Ekman and Wallace V. Friesen, "Constants Across Cultures in the Face and Emotion," *Journal of Personality and Social Psychology* 17, no. 2 (1971): 124–29; P. Ekman and W. V. Friesen, "Nonverbal Leakage and Clues to Deception," *Psychiatry* 32, no. 1 (1969): 88–106; Paul Ekman, E. Richard Sorenson, and Wallace V. Friesen, "Pan-Cultural Elements in Facial Displays of Emotion," *Science* 164, no. 3875 (1969): 86–88  
<https://doi.org/10.1126/science.164.3875.86>; Paul Ekman, Wallace V. Friesen, and Silvan S. Tomkins, "Facial Affect Scoring Technique: A First Validity Study," *Semiotica* 3, no. 1 (1971)
11. Raffi Khatchadourian, "We Know How You Feel," *New Yorker*, January 19, 2015, <http://www.newyorker.com/magazine/2015/01/19/know-feel>.
12. Shoshana Zuboff, *Surveillance Capitalism*, 2016, pp.288-290
13. *ivi*, 278
14. Matthew Rosenberg, Nicholas Confessore, and Carole Cadwalladr, "How Trump Consultants Exploited the Facebook Data of Millions," *New York Times*, March 17, 2018, <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>; Emma Graham-Harrison and Carole Cadwalladr, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach," *Guardian*, March 17, 2018, <http://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>; Julia Carrie Wong and Paul Lewis, "Facebook Gave Data About 57bn Friendships to Academic," *Guardian*, March 22, 2018, <http://www.theguardian.com/news/2018/mar/22/facebook-gave-data-about-57bn-friendships-to-academic>

aleksandr-kogan; Olivia Solon, "Facebook Says Cambridge Analytica May Have Gained 37m More Users' Data," Guardian, April 4, 2018, <http://www.theguardian.com/technology/2018/apr/04/facebook-cambridge-analytica-user-data-latest-more-than-thought>.

15. "Tech Companies Are Pushing Back Against Biometric Privacy Laws," Bloomberg.com, July 20, 2017, <https://www.bloomberg.com/news/articles/2017-07-20/tech-companies-are-pushing-back-against-biometric-privacy-laws>; "Biometric Privacy Laws: Illinois and the Fight Against Intrusive Tech," March 29, 2018, <https://news.law.fordham.edu/jcfl/2018/03/20/biometric-privacy-laws-illinois-and-the-fight-against-intrusive-tech>; April Glaser, "Facebook Is Using an 'NRA Approach' to Defend Its Creepy Facial Recognition Programs," Slate, August 4,

2017, [http://www.slate.com/blogs/future\\_tense/2017/08/04/facebook\\_is\\_fighting\\_biometric\\_fac](http://www.slate.com/blogs/future_tense/2017/08/04/facebook_is_fighting_biometric_fac) Conor Dougherty, "Tech Companies Take Their Legislative Concerns to the States," New York Times, May 27, 2016,

<http://www.nytimes.com/2016/05/28/technology/tech-companies-take-their-legislative-concerns-to-the-states.html>. Deborah D'Souza, "Big Tech Spent Record Amounts on Lobbying Under Trump," Investopedia, July 11, 2017, <https://www.investopedia.com/tech/what-are-tech-giants-lobbying-trump-era>; Brodtkin, "Google and Facebook Lobbyists"; Natasha Lomas, "Google Among Top Lobbyists of Senior EC Officials," TechCrunch (blog), June 24, 2015, <http://social.techcrunch.com/2015/06/24/google-among-top-lobbyists-of-senior-ec-officials/>; "Google's European Revolving Door," Google Transparency Project, September 25, 2017, <http://googletransparencyproject.org/articles/googles-european-revolving-door>.

16. Shoshana Zuboff, *Surveillance Capitalism*, 2016, p.281

17. *ivi*, 255-292

18. Patel, Keyur & Patel, Sunil & Scholar, P & Salazar, Carlos. (2016). *Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges*.

19. E Vitale, F. Cattaneo *Web e società democratica. Un matrimonio difficile*. 2018, pp 18-38

20. *ivi*, pp 34-36

21. *si veda capitolo 1.5*

## 1.5 "The Age of Surveillance Capitalism"

1. Shoshana Zuboff, *Surveillance Capitalism*, 2016, p.63

2. See Lillian Cunningham, “Google’s Eric Schmidt Expounds on His Senate Testimony,” Washington Post, September 30, 2011, [http://www.washingtonpost.com/national/on-leadership/googles-eric-schmidt-expounds-on-his-senate-testimony/2011/09/30/gIQAPyVgCL\\_story.html](http://www.washingtonpost.com/national/on-leadership/googles-eric-schmidt-expounds-on-his-senate-testimony/2011/09/30/gIQAPyVgCL_story.html).
3. Shoshana Zuboff, *Surveillance Capitalism*, 2016, p.103
4. *ivi* 124-127
5. *ivi*, 95
6. EUROPEAN COMMISSION, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, 2018, p. 5  
[https://www.europarl.europa.eu/RegData/docs\\_autres\\_institutions/commission\\_europeenne/com/2018/0795/COM\\_COM\(2018\)0795\\_EN.pdf](https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2018/0795/COM_COM(2018)0795_EN.pdf)
7. Shoshana Zuboff, *Surveillance Capitalism*, 2016, p.82, III “Machine Emotions”, “Sewa Project: Automatic Sentiment Analysis in the Wild,” SEWA, April 25, 2017, <https://sewaproject.eu/description..> Mihkel Jäätma, “Realeyes—Emotion Measurement,” Realeyes Data Services, 2016, [https://www.realeyesit.com/Media/Default/Whitepaper/Realeyes\\_Whitepaper.pdf](https://www.realeyesit.com/Media/Default/Whitepaper/Realeyes_Whitepaper.pdf).
8. Shoshana Zuboff, *Surveillance Capitalism*, 2016, pp 187-192
9. Borsci, S., Lehtola, V.V., Nex, F. et al. Embedding artificial intelligence in society: looking beyond the EU AI master plan using the culture cycle. *AI & Soc* (2022). <https://doi.org/10.1007/s00146-021-01383-> , p. 10
10. [Marco Tulio Ribeiro](#), [Sameer Singh](#), [Carlos Guestrin](#) “Why Should I Trust You?”: Explaining the Predictions of Any Classifier, 2016
11. Borsci, S., Lehtola, V.V., Nex, F. et al. Embedding artificial intelligence in society: looking beyond the EU AI master plan using the culture cycle. *AI & Soc* (2022). <https://doi.org/10.1007/s00146-021-01383-> , p. 14
12. Shoshana Zuboff, *Surveillance Capitalism*, 2016, p 178
13. Shish Shridhar, “We Don’t Need Yet Another App, Conversations Are the New App,” Microsoft Developer Blogs—the ShiSh List, May 21, 2016, <https://blogs.msdn.microsoft.com/shishirs/2016/05/21/we-dont-need-yet-another-app-conversations-are-the-new-app>. Michal Kosinski, David Stillwell, and Thore Graepel, “Private Traits and Attributes Are Predictable from Digital Records of Human Behavior,” *Proceedings of the National Academy of Sciences of the United States of America* 110, no. 15 (2013): 5802–5
14. European Parliamentary Research Service, Author: Marcin Szczepański, *Economic impact of Artificial intelligence (AI) 2019*, pp 4-7
15. Shoshana Zuboff, *Surveillance Capitalism*, 2016, “Make them dance” pp 293-328
16. “Machine Intelligence,” Research at Google, 2018, <https://web.archive.org/web/20180427114330/https://research.google.com/pu>
17. Shoshana Zuboff, *Surveillance Capitalism*, 2016, pp 95-96
18. *ibid.*

19. Xiaoliang Ling et al., “Model Ensemble for Click Prediction in Bing Search Ads,” in Proceedings of the 26th International Conference on World Wide Web Companion, 689–98, <https://doi.org/10.1145/3041021.3054192>.
20. “Schmidt: We Paid \$1 Billion Premium for YouTube,” CNET, March 27, 2018, <https://www.cnet.com/news/schmidt-we-paid-1-billion-premium-for-youtube>.
21. Adrian Covert, “Facebook Buys WhatsApp for \$19 Billion,” CNNMoney, February 19, 2014, <http://money.cnn.com/2014/02/19/technology/social/facebook-whatsapp/index.html>.
22. Shoshana Zuboff, *Surveillance Capitalism*, 2016, p 103
23. Shoshana Zuboff, *Surveillance Capitalism*, 2016, pp 255-293
24. *ivi*, pp 262-264
25. *ivi*, 256
26. *ivi*, 276
27. “See What Industrial Advisors Think About SEWA,” SEWA, April 24, 2017, <https://sewaproject.eu/qa#ElissaMoses>.
28. Rosalind W. Picard, *Affective Computing*, Chapter 3.
29. Picard, *Affective Computing*, 244.
30. “Affective Computing Market by Technology (Touch-Based and Touchless), Software (Speech Recognition, Gesture Recognition, Facial Feature Extraction, Analytics Software, & Enterprise Software), Hardware, Vertical, and Region—Forecast to 2021,” *MarketsandMarkets*, March 2017, <http://www.marketsandmarkets.com/Market-Reports/affective-computing-market-130730395.html>.
31. Joseph Weizenbaum, “Not Without Us,” *SIGCAS Computers and Society* 16, nos. 2–3 (1986): 2–7, <https://doi.org/10.1145/15483.15484>.
32. Satya Nadella et al., “Satya Nadella: Microsoft Ignite 2016,” September 26, 2016, <https://news.microsoft.com/speeches/satya-nadella-microsoft-ignite-2016>.
33. Shoshana Zuboff, *Surveillance Capitalism*, 2016, p 293
34. Hal R. Varian, “Beyond Big Data,” *Business Economics* 49, no. 1 (2014): 6
35. Shoshana Zuboff, *Surveillance Capitalism*, 2016, p 298
36. Bond et al., “A 61-Million-Person Experiment.”
37. Albergotti, “Facebook Experiments Had Few Limits”; Chambers, “Facebook Fiasco.”
38. Darren Davidson, “Facebook Targets ‘Insecure’ to Sell Ads,” *Australian*, May 1, 2017.

## 1.6 IA e ambiente.

1. Anders Nordgren, *Artificial intelligence and climate change: ethical issues*, 2022, p 1

2. Emma Strubell, Ananya Ganesh, Andrew McCallum, Energy and Policy Considerations for Deep Learning in NLP, 2019
3. Roger Harrabin, Google says its carbon footprint is now zero, 14/09/22  
<https://www.bbc.com/news/technology-54141899>
4. Peter Gailhofer, Anke Herold, Jan Peter Schemmel, Cara-Sophie Scherf, Cristina Urrutia, Andreas R. Köhler and Sibylle Braungardt, The role of Artificial Intelligence in the European Green Deal, 2021, pp 30-32
5. Anders Nordgren, Artificial intelligence and climate change: ethical issues, 2022, pp 3-4
6. Emma Strubell, Ananya Ganesh, Andrew McCallum, Energy and Policy Considerations for Deep Learning in NLP, 2019
7. Anders Nordgren, Artificial intelligence and climate change: ethical issues, 2022, p 3
8. *ivi*, p.4
9. *ibid*
10. *ivi*, pp 4-6, Peter Gailhofer, Anke Herold, Jan Peter Schemmel, Cara-Sophie Scherf, Cristina Urrutia, Andreas R. Köhler and Sibylle Braungardt, The role of Artificial Intelligence in the European Green Deal, 2021, pp 22- 27
11. Anders Nordgren, Artificial intelligence and climate change: ethical issues, 2022, p 4
12. *ivi*, p 5
13. *ivi*, pp 6-8
14. David Rolnick<sup>1</sup>, Priya L. Donti<sup>2</sup>, Lynn H. Kaack<sup>3</sup>, Kelly Kochanski<sup>4</sup>, Alexandre Lacoste<sup>5</sup>, Kris Sankaran<sup>6;7</sup>, Andrew Slavin Ross<sup>9</sup>, Nikola Milojevic-Dupont<sup>10;11</sup>, Natasha Jaques<sup>12</sup>, Anna Waldman-Brown<sup>12</sup>, Alexandra Luccioni<sup>6;7</sup>, Tegan Maharaj<sup>6;8</sup>, Evan D. Sherwin<sup>2</sup>, S. Karthik Mukkavilli<sup>6;7</sup>, Konrad P. Körding<sup>1</sup>, Carla Gomes<sup>13</sup>, Andrew Y. Ng<sup>14</sup>, Demis Hassabis<sup>15</sup>, John C. Platt<sup>16</sup>, Felix Creutzig<sup>10;11</sup>, Jennifer Chayes<sup>17</sup>, Yoshua Bengio<sup>6;7</sup>, Tackling Climate Change with Machine Learning, 2019, p. 4 e ss
15. Anders Nordgren, Artificial intelligence and climate change: ethical issues, 2022, p 4
16. *ivi*, p 7
17. *ivi*, p 8
18. *ivi*, pp 8-9
19. *ivi*, p 11
20. Eirini Malliaraki, AI and climate change: The promise, the perils and pillars for action, 2020  
<https://www.climate-kic.org/opinion/ai-and-climate-change-the-promise-the-perils-and-pillars-for-action/>
21. Peter Gailhofer, Anke Herold, Jan Peter Schemmel, Cara-Sophie Scherf, Cristina Urrutia, Andreas R. Köhler and Sibylle Braungardt, The role of Artificial Intelligence in the European Green Deal, 2021, p 36
22. *ivi*, p 37
23. *ivi*, p 39
24. *ibid*.
25. *ibid*

## Capitolo Secondo

### 2. Analisi delle problematiche legate all'uso dell'Intelligenza Artificiale. 2.1 – Il modello LIME

1. [https://it.wikipedia.org/wiki/Modello\\_black\\_box](https://it.wikipedia.org/wiki/Modello_black_box); [Davide Castelvechi](#) Can we open the black box of AI?

Artificial intelligence is everywhere. But before scientists trust it, they first need to understand how machines learn;

Asatiani, Aleksandre; Malo, Pekka; Nagbøl, Per Rådberg; Penttinen, Esko; Rinta-Kahila, Tapani; and Salovaara, Antti (2020) "Challenges of Explaining the Behavior of Black-Box AI Systems," *MIS Quarterly Executive*: Vol. 19: Iss. 4, Article 7. , pp 259-262

[https://pure.itu.dk/ws/portalfiles/portal/85687226/Challenges\\_of\\_Explaining\\_the\\_Behavior\\_of\\_Black\\_Box\\_AI\\_Systems.pdf](https://pure.itu.dk/ws/portalfiles/portal/85687226/Challenges_of_Explaining_the_Behavior_of_Black_Box_AI_Systems.pdf)

2. Asatiani, Aleksandre; Malo, Pekka; Nagbøl, Per Rådberg; Penttinen, Esko; Rinta-Kahila, Tapani; and Salovaara, Antti (2020) "Challenges of Explaining the Behavior of Black-Box AI Systems," *MIS Quarterly Executive*: Vol. 19: Iss. 4, Article 7. , pp 259-262

[https://pure.itu.dk/ws/portalfiles/portal/85687226/Challenges\\_of\\_Explaining\\_the\\_Behavior\\_of\\_Black\\_Box\\_AI\\_Systems.pdf](https://pure.itu.dk/ws/portalfiles/portal/85687226/Challenges_of_Explaining_the_Behavior_of_Black_Box_AI_Systems.pdf)

Borsci, S., Lehtola, V.V., Nex, F. et al. Embedding artificial intelligence in society: looking beyond the EU AI master plan using the culture cycle. *AI & Soc* (2022). <https://doi.org/10.1007/s00146-021-01383-> , p. 10

3. [Marco Tulio Ribeiro](#), [Sameer Singh](#), [Carlos Guestrin](#) "Why Should I Trust You?": Explaining the Predictions of Any Classifier, 2016, p 1

4. Burrell, Jenna. (2016). How the machine 'thinks: Understanding opacity in machine learning algorithms. *Big Data & Society*. 3. 10.1177/2053951715622512., pp 3-5

5. *ivi*, pp 2-3

6. *ivi*, p 8

7. *ivi*, pp 2-3

8. *ibid*

9. *ibid*

10. *ivi*, pp. 8-9

11. *ibid*.

### Capitolo terzo.

3. La normativa vigente nell'Unione Europea e le politiche attuali in materia.

1. European Parliamentary Research Service, Author: Marcin Szczepański, Economic impact of Artificial intelligence (AI) 2019, p 3
2. GDPR, 2016, Art 22 <https://gdpr-info.eu/art-22-gdpr/>;
3. European Commission (2019e) Questions and answers: Coordinated plan for artificial intelligence “made in Europe”. Brussels, 7 December 2019. Available from: [https://ec.europa.eu/commission/presscorner/detail/en/MEMO\\_18\\_6690](https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_6690).
4. European Council, European Convention on Human Right, 1950, Art 8, [https://www.echr.coe.int/Documents/Convention\\_ENG.pdf](https://www.echr.coe.int/Documents/Convention_ENG.pdf)
5. European Union, Directive 95/46/EC , 1995, Artt 1-9 <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046>
6. Carta dei diritti fondamentali dell'Unione Europea, Art 8 [https://www.europarl.europa.eu/charter/pdf/text\\_en.pdf](https://www.europarl.europa.eu/charter/pdf/text_en.pdf)
7. GDPR, 2016, Art 5 <https://gdpr.eu/article-5-how-to-process-personal-data/>
8. *ivi*, Artt 5-50, <https://gdpr.eu/article-5-how-to-process-personal-data/>
9. *ivi*, Artt 44-50
10. *ivi*, Art 25
11. *ivi*, Art 17
12. *ivi*, Art 22; Goodman, B., & Flaxman, S. (2017). European Union Regulations on Algorithmic Decision-Making and a “Right to Explanation”. *AI Magazine*, 38(3), 50-57. <https://doi.org/10.1609/aimag.v38i3.2741>
13. *ibid*, *ibid*
14. Goodman, B., & Flaxman, S. (2017). European Union Regulations on Algorithmic Decision-Making and a “Right to Explanation”. *AI Magazine*, 38(3), 50-57. <https://doi.org/10.1609/aimag.v38i3.2741>, pp 55-56
15. *ibid*
16. *ivi*, p 53
17. *ivi*, p 54
18. *ivi*, p 53-53, “Nondiscrimination”
19. Ulnicane, Inga. (2022). Artificial intelligence in the European Union: Policy, ethics and regulation. 10.4324/9780429262081-19. p 258-59

20. *ivi*, p 258
21. *ibid.*
22. *ibid*
23. *ibid*
24. *ivi*, p 259
25. *ivi*, pp 260-262
26. *ivi*, p 261
27. *ibid*
28. *ivi*, 262
29. *ibid*
30. *ivi*, pp 262-263
31. *ivi*, p 263
32. T. Madiega, S. Chahri, European Parliamentary Research Service, 2022  
[https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS\\_BRI\(2021\)698792\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf)  
Sussman, Schroder, Yavoski, The New EU Approach to the Regulation of Artificial Intelligence, 2021  
<https://www.orrick.com/en/Insights/2021/05/The-New-EU-Approach-to-the-Regulation-of-Artificial-Intelligence>
33. T. Madiega, S. Chahri, European Parliamentary Research Service, 2022, pp 2-3
34. *ivi*, p 4
35. *ibid*
36. *ivi*, pp 5-7
37. *ibid*
38. *ivi*, p 4
39. *ivi*, p 2
40. Ulnicane, Inga. (2022). Artificial intelligence in the European Union: Policy, ethics and regulation. 10.4324/9780429262081-19, p 263
41. Borsci, S., Lehtola, V.V., Nex, F. et al. Embedding artificial intelligence in society: looking beyond the EU AI master plan using the culture cycle. *AI & Soc* (2022). <https://doi.org/10.1007/s00146-021-01383-> , p. 14
42. *ibid*
43. *ibid*
44. [Marco Tulio Ribeiro](#), [Sameer Singh](#), [Carlos Guestrin](#) "Why Should I Trust You?": Explaining the Predictions of Any Classifier, 2016,  
Burrell, Jenna. (2016). How the machine 'thinks: Understanding opacity in machine learning algorithms. *Big Data & Society*. 3. 10.1177/2053951715622512., pp 3-5
45. Borsci, S., Lehtola, V.V., Nex, F. et al. Embedding artificial intelligence in society: looking beyond the EU AI master plan using the culture cycle. *AI & Soc* (2022). <https://doi.org/10.1007/s00146-021-01383-> , p. 14
46. Peter Gailhofer, Anke Herold, Jan Peter Schemmel, Cara-Sophie Scherf, Cristina Urrutia, Andreas R. Köhler and Sibylle Braungardt, The role of Artificial Intelligence in the European Green Deal, 2021, p 37

### 3.2 European Data Strategy

1. European Commission, EU Data Strategy, 2019,

[https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en)

2. European Parliament, The historical development of European integration, 2018

[https://www.europarl.europa.eu/RegData/etudes/PERI/2018/618969/IPOL\\_PERI\(2018\)618969\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/PERI/2018/618969/IPOL_PERI(2018)618969_EN.pdf)

Si veda, cap 1.6, pp. 14-15

3. European Parliament, A European strategy for data, 2021

[https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/690527/EPRS\\_ATA\(2021\)690527\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/690527/EPRS_ATA(2021)690527_EN.pdf)

4. ibid

5. European Commission, Regulation on data governance – Questions and Answers, 2020, p 1

6. ibid

7. ibid

8. ibi, pp 1-2

9. ibid

10. ibid

11. ibid

12. ibid

13. ibid

14. European Commission, Data Act – Questions and Answers, 2022, p 1

15. ibid

16. ibid

17. ibid

18. ibid

19. ibi, p 2

20. ibid

21. ibid

22. ibid

23. ibi, p3

24. ibid

25. ibid

26. ibid

27. ibid

28. ibid

29. ibid

30. ibid

31. Patel, Keyur & Patel, Sunil & Scholar, P & Salazar, Carlos. (2016). Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges.

