

LE PROFONDE IMPLICAZIONI DI CARATTERE ETICO E GIURIDICO DELL'INTELLIGENZA ARTIFICIALE

1. L'intelligenza artificiale: genesi e sviluppo - 2. Il problema della regolamentazione giuridica -
3. I complessi risvolti di carattere etico: la giustizia predittiva - 4. Privacy e sicurezza

Abstract

Il saggio affronta la complessa tematica dell'intelligenza artificiale analizzando le prime applicazioni e le correnti di pensiero che hanno contraddistinto gli ultimi sviluppi dell'IA. Vengono particolarmente approfonditi gli aspetti di natura etica con riferimento specialmente alla giustizia predittiva ed il controverso tema della regolamentazione giuridica che non può prescindere dai naturali riflessi in materia di protezione dei dati personali.

The essay addresses the complex issue of artificial intelligence by analyzing the first applications and currents of thought that have characterized the latest AI developments. The ethical aspects with particular reference to predictive justice and the controversial issue of legal regulation that cannot be separated from the natural reflections on the protection of personal data are particularly studied.

Keywords: Artificial Intelligence, predictive justice, personal data, privacy.

1. L'intelligenza artificiale: genesi e sviluppo

L'aspirazione all'intelligenza artificiale è vecchia quanto la capacità dell'uomo di riflettere su sé stesso, sul mondo che lo circonda e sul suo modo di percepirlo e di modificarlo. Sin da quando ha avuto mezzi tecnici sufficienti, l'uomo si è dedicato alla costruzione di macchine e meccanismi capaci di simulare un comportamento intelligente.

Tuttavia è solo da poco tempo che sono disponibili le tecnologie adeguate per lo sviluppo di sistemi intelligenti così che, quasi simultaneamente, si è giunti nei paesi avanzati a considerare di fondamentale importanza l'intelligenza artificiale ed i *sistemi esperti* in particolare.

Lo studio dell'intelligenza artificiale è senz'altro uno dei campi più stimolanti che si è sviluppato dall'avvento della tecnologia dei computer. Esso coinvolge varie e diverse discipline, come ad esempio la filosofia della mente, la psicologia cognitiva, la linguistica, oltre alla fisica, alla matematica e ad altri campi della scienza e della meccanica relativi specificamente alla realizzazione delle macchine.

Parallelamente agli sviluppi della c.d. informatica "classica", che studia algoritmi e sequenze di istruzioni e procedure, si è sviluppata una ricerca per tentare di simulare ed emulare attraverso i

computer alcuni dei comportamenti ritenuti caratteristici dell'intelletto umano. Questa ricerca ha preso il nome di Intelligenza Artificiale.

In sintesi, l'intelligenza artificiale è quella parte della scienza dei computer riguardante lo studio e la *creazione di sistemi progettati in modo da avere quelle stesse caratteristiche che associamo all'intelligenza umana*: comprensione del linguaggio, capacità di imparare, capacità di risolvere problemi e così via. Le ricerche in questo campo si sono sviluppate già a partire dal 1950, suscitando sia diffidenze per gli eventuali effetti sulla nostra società, sia interesse ed entusiasmo nell'industria informatica. Ciò che in ogni caso si può affermare con certezza è che i programmi d'intelligenza artificiale giocheranno un ruolo importante nell'evoluzione della scienza dei computer.

La logica matematica ha avuto grande rilevanza per lo sviluppo dell'intelligenza artificiale: già i primi sistemi logici di Frege, Russel e Tarski mostrarono che alcuni aspetti del ragionamento logico potevano essere facilmente formalizzati in una struttura. Questo ha continuato ad essere un campo di ricerca dell'intelligenza artificiale anche perché i sistemi logico-deduttivi sono stati sperimentati con successo.

Ma i primi computer erano semplici calcolatori numerici che non avevano nessuna reale intelligenza. Come abbiamo visto in precedenza si deve a studiosi come Church e Turing l'intuizione che i numeri non erano un aspetto essenziale della computazione. In particolare Turing, considerato il padre dell'intelligenza artificiale, inventò un modello di calcolo non numerico, e arguì che il meccanismo di calcolo poteva agire anche in modo intelligente¹.

Per comprendere i fondamenti dell'*intelligenza artificiale* è necessario chiarire la nozione d'*intelligenza naturale* che comprende elementi diversi e di varia complessità. Con quest'ultima locuzione, infatti, deve intendersi quel potenziale innato, di cui è dotato ogni essere umano, necessario per formulare valutazioni giuste, per profittare dell'esperienza e risolvere adeguatamente problemi. L'intelligenza, inoltre, consiste di un insieme di fenomeni con strutture e caratteristiche proprie che rivelano la capacità individuale di selezionare e di organizzare la molteplicità degli aspetti esterni in classi significative in modo da trattare oggetti e situazioni diverse come equivalenti².

¹ Da queste idee si sviluppò, con Turing, Babbage e Von Neumann, la convinzione che fosse possibile progettare e costruire macchine più articolate, capaci di elaborare programmi in grado di svolgere attività più complesse quali, ad esempio, giocare a scacchi o tradurre testi da una lingua ad un'altra.

² Poiché ogni attività conoscitiva è essenzialmente un'attività di classificazione e di presa di significato, si tende ad includere nello studio dell'intelligenza anche quei processi mediante i quali un individuo trae informazioni dall'ambiente, includendovi anche le percezioni, le abitudini e gli adattamenti sensoriomotori elementari. Secondo alcuni autori l'intelligenza è una struttura superiore comprensiva di tutti i processi conoscitivi che essa organizza, pone in equilibrio e potenzia.

Lo studio dell'intelligenza in funzione dell'età, conferma la fondatezza di tale affermazione, la capacità di pensare logicamente, infatti, si sviluppa progressivamente nel bambino. Dapprima essa si basa su azioni sensoriomotorie, poi su rappresentazioni simboliche e, infine, su operazioni logiche; le percezioni e i movimenti sfociano nel pensiero grazie allo sviluppo della capacità di sostituire un'azione o un oggetto mediante un segno (una parola, un segno grafico, un simbolo).

Appare evidente che il concetto d'intelligenza ha molte dimensioni, ma non tutte sono possono essere elaborate nella macchina. Esistono vari tipi d'intelligenza naturale, che è bene distinguere per una maggiore comprensione dell'intelligenza artificiale.

Dalle diverse definizioni e descrizioni dell'intelligenza che si sono succedute nel tempo si può evincere che essa è un insieme di varie capacità come ad esempio: comprendere, classificare, formulare giudizi, ragionare, elaborare concetti, dare risposte appropriate e così via; quindi un sistema, sia esso naturale o artificiale, con una sola di queste capacità è assai limitato. Inoltre la natura multidimensionale dell'intelligenza suggerisce che alcuni elementi saranno più di altri agevolmente strutturabili in sistemi artificiali: è più facile rappresentare elementi in qualche modo quantificabili e misurabili, che elementi di giudizio e di creatività.

Definire quindi l'intelligenza artificiale è arduo quanto definire l'intelligenza naturale e benché molte siano state le definizioni date dai vari studiosi, tutte portano ad una sola conclusione: la ricerca nel settore dell'intelligenza artificiale non può prescindere dai risultati raggiunti dalla ricerca in altre discipline: ad esempio è impossibile far capire al computer un linguaggio naturale senza uno studio della sintassi e della semantica di quel linguaggio.

Ad ogni modo è possibile affermare che gli obiettivi dell'intelligenza artificiale sono essenzialmente due:

- approfondire e comprendere i principi che rendono possibile l'intelligenza (il computer viene usato per simulare le teorie sull'intelligenza);
- progettare computer dotati di capacità simili a quelle umane senza, però, tentare di imitare esattamente i processi informativi degli esseri umani.

I due approcci sono, naturalmente, correlati in quanto il risultato delle ricerche su come la gente risolve i problemi può spesso dare notevoli contributi per le tecniche di *problem-solving* attraverso l'uso dei computer.

Si può tentare di definire l'intelligenza artificiale come quella scienza tendente a sviluppare *modelli computazionali di comportamento intelligente*, in modo che gli elaboratori possano eseguire compiti che richiederebbero intelligenza da parte dell'uomo³.

L'intelligenza artificiale, quindi, comprende, da un lato, la c.d. *scienza cognitiva*, che studia l'intelligenza al fine di rappresentarla in modelli che possano essere trasferiti in applicazioni informatiche, d'altro lato, *l'intelligenza artificiale in senso stretto*, che si occupa delle tecnologie per tali applicazioni. Quest'ultima, a sua volta, è stata divisa in intelligenza *artificiale forte*, intesa a duplicare la mente negli elaboratori, cioè a creare computer in grado di comprendere e di possedere stati cognitivi, ed in *intelligenza artificiale debole* intesa a realizzare sistemi informatici capaci di prestazioni normalmente attribuite all'intelligenza umana, pur senza assumere alcuna analogia tra le menti e i sistemi informatici.

Questa ripartizione dell'intelligenza artificiale è sicuramente la logica conseguenza della duplice concezione dell'intelligenza: quella *pulita* che assume la riducibilità di tutte le manifestazioni dell'intelligenza a pochi principi, esprimibili con eleganza in formalismi logici o matematici e quella *sporca*, secondo la quale, invece, l'intelligenza è una raccolta di molti metodi *ad hoc*, ciascuno adeguato ad un compito specifico.

Il dibattito tra la concezione *sporca* e la concezione *pulita* dell'intelligenza è connesso alla controversia tra i modelli procedurali ed i modelli dichiarativi della conoscenza: i primi assumono che la conoscenza sia costituita da un insieme di procedure intese a raggiungere determinati scopi nell'interazione con l'ambiente; i secondi presuppongono, invece, che la conoscenza consista di asserzioni che rappresentano il contesto dell'azione intelligente.

Le ricerche sulla intelligenza artificiale, come già sostenuto in precedenza, sono state dominate sin dall'inizio, da una nozione determinata di intelligenza che è possibile qualificare come formalistica o razionalistica: *l'intelligenza è stata prevalentemente identificata con l'uso di teorie, cioè di rappresentazioni simboliche della realtà*⁴.

³ Questi compiti possono essere suddivisi in:

- compiti del senso comune, che possono essere svolti da qualsiasi persona adulta normale, anche priva di una formazione specifica (come parlare la propria lingua madre, riconoscere oggetti e forme, comprendere la trama di racconti, ecc.);

- compiti da esperti, che normalmente presuppongono conoscenze e abilità specifiche (come diagnosticare malattie, progettare sistemi informatici, effettuare analisi chimiche, ecc.).

⁴ Si può dire che l'intelligenza artificiale trovi le sue fondamenta nel XVII secolo, ovvero quando Blaise Pascal (scienziato, scrittore e filosofo francese) inventa la cosiddetta Pascalina, strumento precursore della moderna calcolatrice, per aiutare il padre, incaricato dall'amministrazione fiscale della Normandia di eseguire un difficile lavoro di

L'intelligenza artificiale però deve la sua evoluzione necessariamente agli avanzamenti della tecnologia informatica, anche se la parte teorica evolve indipendentemente dai progressi scientifici. Infatti, solo nella seconda metà del XX secolo è possibile poter utilizzare di dispositivi di calcolo e linguaggi di programmazione sufficientemente potenti da permettere sperimentazioni sull'I.A.

I calcolatori raggiungono una struttura maggiormente definita grazie alla sostituzione dei relè, usati per i primi calcolatori elettromeccanici, con le valvole o tubi elettronici.

Nel 1946, si giunge finalmente alla creazione di ENIAC (Electronic Numerical Integrator And Calculator), concepito come calcolatore moderno nel 1945 da John von Neumann. Il compito di ENIAC consisteva nell'elaborazione a lotti (batch) nell'ordine di migliaia di informazioni al minuto e la programmazione avveniva comunque tramite schede.

Un ulteriore salto nella programmazione dei calcolatori, ovvero l'avvento della seconda generazione di computer, si ha negli anni '60, con il time sharing, cioè sistemi basati sulla divisione di tempo e quindi maggiormente veloci. In pratica, si hanno più terminali, la maggior parte telescriventi, collegati ad un calcolatore centrale e soprattutto il passaggio dalle valvole ai transistor, che è l'innovazione più significativa.

A quell'epoca i programmi erano fortemente condizionati dai limiti dei linguaggi di programmazione, oltre che dai limiti di velocità e memoria degli elaboratori. Il mutamento radicale si ha proprio tra gli anni '50 e '60, con linguaggi di manipolazione simbolica come l'ILP, il LISP e il POP. Un punto di svolta nella storia dell'intelligenza artificiale si ha con la famosa pubblicazione nel 1950 di un articolo da parte di Alan Turing, sulla rivista *Mind*.

Nello stesso anno in cui Turing pubblica il suo articolo sul test per le macchine pensanti, Arthur Samuel presenta il primo programma capace di giocare a dama, che è un risultato molto importante perché dimostra la possibilità di superare i limiti tecnici (il programma era scritto in

calcolo. La macchina era in grado di eseguire automaticamente addizione e sottrazione; questa "macchina aritmetica" fu la capostipite dei calcolatori ad ingranaggi.

In età vittoriana, Charles Babbage creò macchine calcolatrici a rotelle, la cosiddetta "The difference engine" (la macchina alle differenze), che era capace di fare calcoli differenziali ed arrivò a progettarne addirittura una intelligente che però, per problemi tecnici e pratici, non riuscì mai a funzionare, in quanto avrebbe dovuto essere progettata con schede perforate, un po' come accadde in seguito con i primi calcolatori.

Hermann Hollerith (statistico americano di origine tedesca) inventò le schede perforate applicate a calcolatrici attorno al 1885 e questo sistema fu usato per la prima volta per i calcoli relativi all'11° censimento americano, nel 1891.

Le schede perforate, cartoncini forati a secondo della necessità, furono ampiamente usati per esempio per il funzionamento dei telai Jacquard, di pianole meccaniche, quindi dei primi calcolatori. Il sistema meccanografico adottato da Hollerith riscosse tale successo da indurlo a fondare la Tabulating Machine corporation. In seguito i calcolatori furono molto usati dai militari per regolare il tiro dell'artiglieria.

Assembly e girava su un IBM 704) per realizzare sistemi capaci di risolvere problemi tradizionalmente legati all'intelligenza umana. Inoltre, la cosa più sorprendente è che l'abilità di gioco viene appresa dal programma scontrandosi con avversari umani.

Nel 1956, alla conferenza di Dartmouth, il workshop in cui viene utilizzata per la prima volta la terminologia "intelligenza artificiale", vengono mostrati due programmi che segnano un'altra importante tappa dello sviluppo dell'IA. I programmi, che furono sviluppati dagli studiosi Allen Newell, J. Clifford Shaw e Herb Simon, erano i cosiddetti "Logic Theory Machine" e "General Problem Solver" (GPS). Il GPS rappresenta forse il primo tentativo di separare la strategia di problem solving dall'informazione sui problemi da risolvere. Ambedue i programmi furono sviluppati usando il linguaggio Information Processing Language (IPL) sviluppato dai tre ricercatori dell'intelligenza artificiale nello stesso anno.

La linea seguita dalla giovane intelligenza artificiale si basa quindi sulla ricerca di un automatismo nella creazione di un'intelligenza meccanica. L'approccio segue essenzialmente un'euristica di ricerca basata su tentativi ed errori oltre che investigare su tecniche di apprendimento efficaci.

Dopo il 1962, l'intelligenza artificiale, come ci testimoniano le parole di Marvin Minsky, cambia le sue priorità: essa si interessa di meno all'apprendimento per concentrarsi maggiormente sulla rappresentazione della conoscenza e sul problema ad essa connesso del superamento del formalismo finora a disposizione e liberarsi dalle costrizioni dei vecchi sistemi⁵.

I ricercatori dediti allo studio e allo sviluppo dell'intelligenza artificiale si specializzarono soprattutto nell'elaborazione del linguaggio naturale, che appare essere un campo destinato a un rapido sviluppo. La traduzione diretta di testi porta però ad insuccessi che influenzeranno per molti anni i finanziamenti in tale campo. Malgrado ciò, viene dimostrato abbastanza presto che si possono ottenere buoni risultati in contesti limitati.

⁵ La ricerca, che si indirizza su quanto precedente detto, si basa sugli studi di Marvin Minsky sulla rappresentazione distribuita della conoscenza, la cosiddetta "società delle menti", e sul lavoro di John McCarthy riguardo la rappresentazione dichiarativa della conoscenza. Quest'ultima viene espressa formalmente mediante estensioni della logica dei predicati e può quindi essere manipolata facilmente. Con i suoi studi sul ragionamento non monotono e di default, McCarty contribuisce a porre gran parte delle basi teoriche dell'IA.

Il punto di vista psicologico non viene assolutamente trascurato. Ad esempio il programma EPAM, che prende corpo nel 1963 dalle menti di Feigenbaum e Feldman, esplora la relazione tra memoria associativa e l'atto di dimenticare; mentre, negli stessi anni, alla Carnegie Mellon University vengono sperimentati programmi per riprodurre i passi del ragionamento, inclusi eventuali errori.

Nei primi anni '70, si sviluppano i sistemi di produzione, cioè dei programmi che sfruttano un insieme di conoscenze organizzate in base di dati, attraverso l'applicazione di regole di produzione, per ottenere risposte a domande precise. Però questi vennero presto sostituiti dai sistemi esperti a causa delle difficoltà incontrate dai sistemi di produzione, soprattutto in merito alla necessità di fornire inizialmente la conoscenza in forma esplicita e la poca flessibilità delle regole di produzione. I sistemi esperti, di cui *Dendral* è il più rappresentativo, manifestano le enormi possibilità offerte da un valido sfruttamento di poche basi di conoscenza per programmi capaci di prendere decisioni o fornire avvisi in molte aree diverse: l'analisi dei dati viene razionalizzata e generalizzata.

Però, nello studio dell'intelligenza artificiale, avanza il problema del trattamento dell'incertezza, che è parte costituente della realtà e delle problematiche più comuni. In merito a ciò, Mycin introduce l'uso di "valori di certezza", ovvero un numero associato a ciascun dato e che viene calcolato per la nuova conoscenza inferita.

Malgrado ciò, le difficoltà nel trattare correttamente l'incertezza portano ad abbandonare l'uso di sistemi a regole per avvicinarsi a quella che è la moderna IA.

Le attività intelligenti si basano su un impiego attivo, non rigidamente predeterminato, della conoscenza. Di qui l'esigenza di sviluppare un nuovo tipo di sistemi informatici, i cosiddetti sistemi basati sulla conoscenza, mediante i quali ci si propone di usare in modo intelligente le informazioni, trasformando i dati in conoscenza.

I programmi informatici tradizionali, pur non essendo basati sulla conoscenza, ne incorporano una, essi difatti non sono altro che la descrizione della procedura (l'algoritmo), per svolgere un certo compito, e possono essere sviluppati solo tenendo conto delle caratteristiche di quel compito. È possibile delineare delle differenze tra i sistemi informatici tradizionali e quelli basati sulla conoscenza.

Nei sistemi informatici tradizionali:

1. La conoscenza non è mai rappresentata esplicitamente e non è mai separata dalle procedure che la usano e che ne disciplinano l'elaborazione;
2. la conoscenza è applicata in modo rigidamente predeterminato;
3. non è possibile aggiungere nuova conoscenza senza modificare le procedure;
4. il sistema non è in grado di esporre la conoscenza sulla quale si basa né di spiegare perché, sulla base della stessa, sia giunto a determinati risultati.

Invece, nei sistemi basati sulla conoscenza:

1. La conoscenza è contenuta in una determinata base, dove è rappresentata in un linguaggio ad alto livello, cioè in una forma relativamente vicina al linguaggio usato nella comunicazione umana. È possibile adottare una rappresentazione dichiarativa del compito affidato al sistema informatico, lasciando al sistema l'individuazione della procedura da seguire per svolgere quel compito;

2. la conoscenza è usata da un *motore inferenziale*, ovvero un meccanismo in grado di interpretare il contenuto della base di conoscenza ed effettuare deduzioni logiche in modo da risolvere il problema posto al sistema;

3. la base di conoscenza può essere arricchita di nuove informazioni senza intervenire sul motore inferenziale;

4. il sistema è in grado di esporre in forma comprensibile le premesse e le inferenze che hanno condotto ad un determinato risultato, cioè di giustificare le conclusioni cui giunge.

I sistemi basati sulla conoscenza sono spesso completati da interfacce che agevolano l'interrogazione e la preparazione della base della conoscenza.

In definitiva essi sono costituiti da tre componenti fondamentali:

- la base di conoscenza;
- il motore inferenziale;
- le interfacce, rivolte tanto all'utente quanto all'ingegnere della conoscenza (autore del programma).

Il *sistema esperto* non è altro che un sistema basato sulla conoscenza in grado di eseguire compiti che richiedono conoscenza specializzata, possono essere svolti solo da esperti o da persone dotate di notevoli competenze. Il sistema esperto è quindi composto da due elementi:

- un elemento *strutturale*, in ragione del quale il sistema è basato sulla conoscenza, cioè si compone di una base di conoscenza distinta dal motore inferenziale;
- un elemento *funzionale*, in ragione del quale il sistema deve essere in grado di fornire prestazioni che richiedano notevoli competenze.

I sistemi esperti sono programmi in cui l'utente interagisce in un dialogo simile a quello che si svolgerebbe con un esperto umano, al quale è stato esposto un problema ed al quale vengono rivolte domande sulle soluzioni proposte. Tali sistemi possono essere visti come intermediari tra gli

esperti umani, che interagiscono con il sistema nell'acquisire conoscenza, e l'utente umano che interagisce con il sistema nella consultazione⁶.

In generale, la caratteristica fondamentale di un sistema esperto dovrebbe essere in primo luogo quella di essere in grado di simulare il ragionamento che un esperto umano farebbe in quelle determinate circostanze; le soluzioni date dal sistema dovrebbero essere della stessa qualità ed inoltre prospettate con una maggiore rapidità, altrimenti non si giustificerebbe l'apporto informatico.

Altra caratteristica importante è che il sistema sia capace di spiegare e giustificare il suo procedimento. Generalmente il sistema interagisce con l'utente attraverso domande a cui l'utente stesso può tanto rispondere con sì o no o non rispondere perché non possiede la relativa informazione o perché non ha compreso la domanda. Un buon sistema esperto, nel primo caso, deve poter porre altre domande alternative per giungere comunque ad un risultato; nel secondo caso, l'utente deve poter chiedere delle delucidazioni sulla domanda. Questo differenzia i sistemi esperti dai tradizionali sistemi a dialogo; infatti il sistema esperto può agire anche su informazioni incerte o incomplete, cercando di ricavare l'informazione per strade diverse. In sedute particolarmente lunghe in cui l'utente può perdere il filo del ragionamento e quindi non capire il nesso tra la domanda attuale e quelle precedenti, si può porre al sistema la domanda "perché?" forzando il sistema a spiegare la linea di ragionamento seguita, le deduzioni che ha tratto da solo e, così, la giustificazione della domanda posta; è anche necessario dotare il sistema della capacità di giustificare o spiegare come è giunto ad una determinata soluzione, perché l'utente può non aver compreso la conclusione finale o una delle intermedie.

In sintesi, i principali attributi che si riconoscono ai sistemi esperti e che derivano dalle loro caratteristiche sono:

1. *la trasparenza*, ovvero la possibilità di fornire spiegazioni circa le linee di ragionamento seguite per raggiungere la o le conclusioni;
2. *l'euristica*, cioè l'adozione di strategie tipiche degli esperti umani;
3. *la flessibilità*, ovvero la capacità di seguire, senza grosse difficoltà, modificazioni alle loro basi di conoscenza cioè alla loro riserva di conoscenza.

⁶ La ricerca in questo campo dell'intelligenza artificiale ha anche cercato di dotare questi sistemi della possibilità di spiegare il loro ragionamento, sia per rendere semplice la consultazione per l'utente, sia per aiutare l'esperto a rilevare eventuali errori nel ragionamento del sistema.

Ultimamente però i sistemi esperti sono stati affiancati nell'ambito dell'intelligenza artificiale applicata al diritto dalle c.d. reti neurali. Difatti, il dibattito delle scienze cognitive è tutt'oggi aperto, ponendo in dubbio l'esistenza di un sistema simbolico mentale quale causa dei processi cognitivi, ed attribuendo ad esso il ruolo di procedimento euristico, mezzo per la predizione dei comportamenti quotidiani della persona. Il sistema simbolico viene concepito come un modello adatto a descrivere grossolanamente e macroscopicamente il comportamento umano, non però il suo reale funzionamento a livello neuronale.

Le reti neurali differiscono in modo radicale e per diversi aspetti dai tradizionali modelli di intelligenza artificiale. Le principali differenze derivano dal presupposto che le reti apprendono, non conoscono già le regole ma si modellano, attraverso un algoritmo di apprendimento, in modo tale da comportarsi come se conoscessero le regole, alla fine dell'apprendimento. Quale sarà il risultato finale del procedimento d'apprendimento è imprevedibile per il programmatore stesso: il programmatore non può prevedere l'evoluzione della rete. Ma una volta terminato l'apprendimento la rete diventa stabile e la sua configurazione non cambia più.

Si può quindi definire la rete neurale artificiale (ANN – artificial neural network – nella letteratura in lingua inglese) come una replica artificiale (hardware o simulata via software) delle reti neurali naturali, quelle biologiche, cioè dell'insieme delle cellule (i cosiddetti neuroni) che costituiscono il cervello umano o animale; gli studi hanno dimostrato che un determinato tipo di reti neurali artificiali, quelle con apprendimento supervisionato, a differenza dei normali computer che devono essere programmati con procedure algoritmiche, sono in grado di individuare la soluzione di problemi che vengono loro posti, apprendendo direttamente dall'esperienza che accumulano presentando loro ripetutamente una serie di esempi del problema da trattare, corredati delle relative soluzioni.

Esse simulano quindi il funzionamento del cervello umano e animale, che riesce a trovare la soluzione ai vari problemi semplicemente basandosi sull'esperienza del passato. Le reti neurali artificiali si inseriscono in qualche modo nell'ampia tematica dell'intelligenza artificiale e ne costituiscono un'evoluzione innovativa; è innegabile che lo stimolo alla realizzazione delle reti neurali artificiali provenga dal desiderio di riprodurre sistemi di elaborazione "intelligenti", simili, per prestazioni e comportamento, all'uomo, le cui azioni sono governate dal cervello.

Questo organo è costituito per la maggior parte da cellule, così come le altre parti del corpo umano, e rispecchia in via generale la teoria cellulare di Rudolf Virchow; le cellule del cervello sono chiamate cellule nervose o neuroni.

Le reti neurali artificiali replicano l'organizzazione del cervello umano, essendo costituite da molti processori semplici (neuroni artificiali) interconnessi fra sé. Ogni neurone artificiale, in modo sostanzialmente simile ad un neurone biologico, calcola il segnale in uscita come funzione della differenza fra il prodotto dei segnali di entrata per i rispettivi pesi sinaptici, ed un valore di soglia prefissato.

A livello complessivo le reti neurali artificiali ricordano nelle loro prerogative il cervello (umano o animale) essenzialmente per due aspetti:

- la conoscenza è acquisita attraverso un progressivo processo di apprendimento, e non è immessa tutto ad un tratto dall'esterno come invece avviene per i computer tradizionali;
- la forza delle connessioni fra neuroni, conosciuta anche come peso sinaptico, è utilizzata per immagazzinare la conoscenza e per l'apprendimento⁷.

Perché ricorrere ad una rete neurale? Quali sono i vantaggi?

Gli indiscutibili vantaggi che una rete neurale artificiale fornisce rispetto agli ordinari metodi sono da vedersi principalmente in campo previsionale, difatti:

- è possibile operare previsioni efficienti anche nel caso di mancanza di una variabile di input in quanto la rete tollera la mancanza di alcuni dati essenziali;
- è possibile inserire fra le variabili di input anche variabili che non hanno influenza sul fenomeno in esame. La rete provvederà da sola a non prendere in esame, o a prenderle in esame nella misura dovuta, le variabili di input che non hanno influenza o che hanno influenza limitata sul fenomeno. Grazie a questo è possibile, in caso di dubbio sull'importanza o meno di una determinata variabile per il fenomeno che viene considerato, fornire comunque alla rete anche i dati corrispondenti alla variabile dubbia, senza per questo avere previsioni scorrette;
- non sono necessarie conoscenze matematiche particolarmente approfondite; tutto quello che è necessario, oltre alla padronanza della tematica delle reti neurali artificiali, è un po' di attenzione

⁷ La ricerca nel campo della intelligenza artificiale si è indirizzata verso l'imitazione del sistema nervoso, ritenendo che fosse questo il modello più valido di funzionamento, operando su due versanti complementari:

- da una parte, cercando di costruire macchine informatiche simili al cervello umano, nella speranza che avrebbero avuto potenzialità superiori alle macchine attuali;
- dall'altra, nell'utilizzare modelli di programmazione e di ragionamento simili a quelli umani, ma facendoli funzionare sulle attuali macchine informatiche.

Oggigiorno le reti neurali artificiali sono utilizzate in svariate applicazioni pratiche, per lo più in ambito finanziario (per prevedere l'evoluzione dei titoli di borsa), industriale (come nel riconoscimento di pattern, nel controllo di processi), o anche casalingo (nel riconoscimento vocale utilizzato dai telefoni cellulari, nel riconoscimento dei caratteri utilizzato dagli scanner); al momento sono invece ancora molto limitate le applicazioni nel nostro specifico settore.

nella costruzione della rete (individuazione del tipo, dell'architettura, del numero dei nodi) e quindi molta pazienza nell'ottimizzare i parametri di lavoro della rete rispetto allo specifico fenomeno.

2. Il problema della regolamentazione giuridica

Lo sviluppo dell'IA ed anche l'introduzione della robotica creeranno inevitabilmente non pochi problemi dal punto di vista sia etico che giuridico poiché normative eccessivamente rigide potrebbero soffocare l'innovazione, ma la mancanza di chiarezza giuridica lascerebbe tutti gli operatori nel buio. Si pensi, ad esempio, ai sistemi bionici umani, cioè ad una serie di tecnologie (che vanno da protesi bioniche a esoscheletri alle protesi del corpo alle interfacce cervello-computer), che consentirà di ripristinare le funzioni corporee perse e alla fine superare diversi tipi di disabilità, la cui distribuzione, però, pone problemi più generali per quanto riguarda l'impatto sulle nozioni di natura umana, identità, normalità, disabilità, ed i corrispondenti effetti giuridici⁸.

Un contesto normativo trasparente, è visto come un elemento chiave per lo sviluppo della di sistemi informatici intelligenti di mercato, in cui prodotti e servizi possono essere distribuiti senza problemi. C'è il forte timore da parte di molti che una legislazione prematura ed invadente possa ostacolare il progresso scientifico ed annullare potenziali vantaggi o peggio ancora causare inefficienze economiche o altro. Allo stesso tempo, in qualche modo paradossalmente, si ammette che la mancanza di un ambiente giuridico affidabile e sicuro possa ugualmente ostacolare l'innovazione tecnologica. Tale difficile situazione mina sicuramente la certezza del diritto ed induce la gente ad agire in un settore ambiguo in cui i diritti e le responsabilità non sono preventivamente individuabili.

Indubbiamente un intervento normativo si renderà necessario quanto meno per ottenere un quadro giuridico che sia in grado di supportare un costante progresso scientifico senza mai porsi come ostacolo allo sviluppo tecnologico.

Leggi e regolamenti nel settore dell'IA saranno fondamentali anche per consentire un effettivo sviluppo di un mercato competitivo. L'ambizione dell'Unione europea di promuovere l'innovazione nel mercato interno fa dell'IA un settore strategico, a cui le istituzioni europee stanno dedicando una notevole attenzione. Allo stesso tempo la ricerca e la produzione industriale nel campo della stessa intelligenza artificiale e della robotica devono crescere in linea con l'obiettivo

⁸ Situazioni simili le possiamo trovare quando le tecnologie in gioco sono veicoli autonomi, robot software distribuiti nella finanza moderna, tecnologie robotiche destinate ad essere utilizzate in ambito sanitario.

complementare, che è sancito dalla politica europea, di affermarsi come uno spazio di libertà, sicurezza e giustizia.

Gli obiettivi concorrenti di proteggere i consumatori e più in generale gli utenti finali da effetti pregiudizievoli promuovendo contemporaneamente l'innovazione devono quindi diventare propri del legislatore. A questo proposito, il sistema normativo più efficace deve combinare più strumenti: norme giuridiche, norme e standard tecnici, codici di condotta e best practices. In questo modo sarà possibile garantire la certezza, la flessibilità, la precisione ed anche l'interpretazione più corretta di fronte a determinati dubbi.

Un problema spesso sottolineato quando si affronta la tematica del rapporto tra tecnologia e regolamentazione è la lentezza della legge, nel senso che l'innovazione tecnologica è molto più rapida del legislatore che interviene con notevole ritardo a regolare l'introduzione di determinati prodotti o servizi di alto contenuto tecnologico (si pensi ad esempio ai droni). Il problema giuridico si pone non solo quando nasce una nuova tecnologia emergente ma anche quando ci troviamo di fronte a profonde trasformazioni di tecnologie già esistenti. In questo caso nasce l'esigenza di adattare un quadro normativo preesistente al continuo evolversi del progresso tecnologico.

Gli uffici del futuro saranno più interattivi, collaborativi e semplificati rispetto a quelli di oggi, e il merito sarà delle tecnologie e dei processi che creeranno modalità di lavoro diverse. Le innovazioni che entro i prossimi vent'anni potranno colonizzare gli uffici includono i droni, le comunicazioni Bluetooth cervello-cervello e i trasmettitori sensoriali (piccoli dispositivi da inserire nell'orecchio, che inviano dati audio e video al cervello sotto forma di segnali elettronici). Sono ormai ipotizzabili robot che fungono da "assistenti", immagazzinando informazioni e apprendendo dall'esperienza e dall'osservazione della realtà, oppure un customer service totalmente automatizzato. Un altro tipo di assistente virtuale, in questo caso non basato su hardware ma totalmente incorporeo, potrebbe nascere dall'utilizzo di ologrammi. Oppure, perché no, gli ologrammi potrebbero in certi casi sostituire i colleghi in carne e ossa, lontani oppure assenti dall'ufficio. Se tutto questo sembra ancora troppo futuristico per poterlo immaginare, si pensi a un acquisto recente del distretto del Brent, nel Regno Unito, che ha speso 12mila sterline per "Shanice"⁹: un'avvenente assistente virtuale che, proiettata su un muro della sede del consiglio distrettuale, fornisce indicazioni e risponde alle domande dei visitatori.

⁹ <https://www.standard.co.uk/news/techandgadgets/say-hello-to-shanice-brent-councils-12000-hologram-greeter-8773655.html>

La ricerca sulla IA e la relativa regolamentazione rappresenta un costante punto di riferimento per le politiche comunitarie in materia di innovazione. Le principali questioni sono state affrontate sia da un punto di vista metodologico che da un punto di vista sostanziale. Da un lato, infatti, l'approccio interdisciplinare è stata una caratteristica costante dello studio fin dal suo inizio. L'esperienza diversificata dei ricercatori coinvolti (avvocati, filosofi, ingegneri, ecc.) hanno portato ad una costante interazione finalizzata allo scambio di informazioni, opinioni e punti di vista in modo che le regole suggerite fossero il risultato di una complessa valutazione tecnica, etica e giuridica.

Non bisogna dimenticare che le nuove tecnologie hanno spesso effetti dirompenti, imponendo cambiamenti radicali nello stile di vita, nell'economia e nel comportamento sociale delle persone, per cui la discussione sui benefici e sui pericoli delle nuove tecnologie è sempre molto accesa. La tecnologia solitamente viene definita neutrale, ma è l'uomo che decide se usarla per scopi buoni o cattivi.

Esiste, quindi, un problema di educazione sociale e consapevolezza sociale, che non serve solo ad indirizzare il comportamento umano nella direzione corretta, ma anche a mantenere alta l'attenzione sui pericoli che non sono intrinseci ad una tecnologia in sé ma che possono derivare dai suoi utilizzi impropri o effetti inattesi¹⁰.

3. I complessi risvolti di carattere etico: la giustizia predittiva

Ci sono alcuni temi ricorrenti di carattere etico sui quali vale la pena soffermarsi.

Il primo è senz'altro quello legato a future tecnologie intelligenti che potrebbero un giorno rimpiazzare l'umanità: il robot intelligente, dotato di un'intelligenza artificiale così sviluppata da entrare in conflitto con gli umani, sino a volerli sostituire. In realtà questa prospettiva è piuttosto ambiziosa poiché nessun robot, probabilmente, avrà mai quel complesso sistema biochimico che governa il comportamento ormonale degli esseri umani. Aggressività, euforia, rabbia, gioia, tristezza sono manifestazioni tipicamente umane che nascono da una biochimica sofisticatissima che difficilmente potrà essere trasferita alle macchine. Il giorno in cui questo fosse possibile, non avremo più robot, ma cloni e allora di certo sorgeranno questioni etiche immense, ma non connesse alla robotica bensì alla genetica della duplicazione umana.

¹⁰ R. CINGOLANI, G. METTA, *Umani e umanoidi*, Bologna, 2015.

Un secondo argomento di riflessione riguarda il timore dell'isolamento progressivo dell'essere umano, che potrebbe un giorno avere più contatti con il proprio personal computer particolarmente evoluto che con i propri simili. È interessante l'analogia con le moderne tecnologie di comunicazione: se da un lato l'accesso ad Internet mediante la telefonia mobile ha permesso a tutti di entrare in comunità digitali costituite da miliardi di persone, creando l'illusione di un'immensa società digitale, dall'altro ha sollevato il rischio di un isolamento individuale, spesso esemplificato da tristissime immagini di umani che, invece di parlarsi, stanno ripiegati sui propri touch screen. Nel caso specifico, in effetti, la presenza di un sistema autonomo aggiungerà un terzo livello.

Tenendo conto dell'importanza dell'intelligenza artificiale, la CEPEJ Commissione Europea per l'Efficacia della Giustizia¹¹, il 4 dicembre 2018¹², ha emanato la *Carta etica europea sull'utilizzo dell'intelligenza artificiale*. Si tratta di un documento di eccezionale rilevanza, poiché è la prima volta che a livello europeo, preso atto della «crescente importanza della intelligenza artificiale (IA) nelle nostre moderne società e dei benefici attesi quando questa sarà pienamente utilizzata al servizio della efficienza e qualità della giustizia», vengono individuate alcune fondamentali linee guida, alle quali dovranno attenersi «i soggetti pubblici e privati responsabili del progetto e sviluppo degli strumenti e dei servizi della IA». La Cepej rileva fin dall'inizio che l'uso di strumenti e servizi di IA nei sistemi giudiziari è volto a migliorare l'efficienza e la qualità della giustizia e merita di essere incoraggiata. Tuttavia, ciò deve avvenire in modo responsabile, nel rispetto dei diritti fondamentali sanciti dalla Convenzione europea dei diritti dell'uomo (Cedu) e dalla Convenzione n. 108 del Consiglio d'Europa¹³ sulla protezione dei dati personali, nonché degli altri principi fondamentali

¹¹ www.intelligenzaartificialeegiustiziadelgiudice.it

¹² www.questionegiustizia.com. La Carta etica europea sull'uso dell'intelligenza artificiale (IA) nei sistemi giudiziari e in ambiti connessi è il primo strumento europeo e mondiale che stabilisce cinque principi sostanziali e metodologici che si applicano al trattamento automatizzato delle decisioni e dei dati giudiziari, sulla base di tecniche di IA. Sviluppato dalla Commissione europea per l'efficienza della giustizia (Cepej) del Consiglio d'Europa, si rivolge alle imprese private (start-up attive sul mercato delle nuove tecnologie applicate ai servizi legali-legaltechs) e ai soggetti pubblici incaricati della progettazione e dell'implementazione di strumenti e servizi di IA in questo campo. Si rivolge anche alle autorità pubbliche responsabili dell'elaborazione di strumenti legislativi o regolamentari, dello sviluppo, dell'audit o dell'uso di tali strumenti e servizi, nonché agli operatori del diritto.

¹³ Convenzione numero 108 del Consiglio d'Europa. La Convenzione rappresenta il primo strumento internazionale obbligatorio che ha per scopo la protezione delle persone contro l'uso abusivo del trattamento automatizzato dei dati di carattere personale, e che disciplina il flusso transfrontaliero dei dati. Oltre le garanzie previste per il trattamento automatizzato dei dati di carattere personale, essa bandisce il trattamento dei dati «delicati» sull'origine razziale, sulle opinioni politiche, la salute, la religione, la vita sessuale, le condanne penali, in assenza, di garanzie previste dal diritto interno. La Convenzione garantisce anche il diritto delle persone di conoscere le informazioni catalogate su di loro ed ad esigere, se del caso, delle rettifiche.

enunciati nella Carta. Tra questi principi, il rispetto dei diritti umani e la non discriminazione sono di fondamentale importanza. L'obiettivo è garantire, dalla fase di progettazione fino all'applicazione pratica, che le soluzioni garantiscano il rispetto dei diritti garantiti dalla Cedu e dalla Convenzione n. 108 del Consiglio d'Europa. Di grande importanza è anche il principio della trasparenza delle metodologie e delle tecniche utilizzate nel trattamento delle decisioni giudiziarie. L'accento è posto sull'accessibilità e la necessità di comprensione delle tecniche di trattamento dei dati, nonché sulla possibilità per le autorità o gli esperti indipendenti di effettuare audit esterni. Viene inoltre incoraggiato un sistema di certificazione, da rinnovare regolarmente. In particolare, in ambito giudiziario, il giudice dovrebbe poter controllare in qualsiasi momento le decisioni giudiziarie e i dati che sono stati utilizzati per produrre un risultato e continuare ad avere la possibilità di discostarsi dalle soluzioni proposte dall'IA, tenendo conto delle specificità del caso in questione. Ogni utente dovrebbe essere informato, in un linguaggio chiaro e comprensibile, della natura vincolante o non vincolante delle soluzioni proposte dagli strumenti di IA, delle diverse opzioni disponibili e del loro diritto all'assistenza di un avvocato e al ricorso a un tribunale. Sintetizzando, in modo particolare, questa carta quindi, si avvale di cinque principi di fondamentale importanza:

1. Principio del rispetto dei diritti fondamentali;
2. Principio di non discriminazione;
3. Principio di qualità e sicurezza;
4. Principio di trasparenza, imparzialità e equità;
5. Principio del controllo da parte dell'utilizzatore.

La Corte Superiore di Giustizia di Buenos Aires¹⁴, attraverso l'utilizzo di un software, ha risolto più di mille casi nell'arco di sette giorni, a fronte degli ottantatré giorni che gli occorrevo precedentemente¹⁵. Lo stesso software è in corso di sperimentazione presso il Consiglio di Stato di Parigi¹⁶. Il tema dell'efficienza della giustizia, è un tema che da anni abbraccia la nostra nazione, ma in modo particolare conferisce una stringente attualità a quello della giustizia predittiva¹⁷, ossia la

Unica restrizione a tale diritto può aversi solo in caso in cui sia presente un interesse maggiore (sicurezza pubblica, difesa, etc.). La Convenzione impone anche delle limitazioni ai flussi transfrontalieri di dati negli stati in cui non esiste alcuna protezione equivalente.

¹⁴ www.ilcorrieredelasera.it

¹⁵ www.giustiziapredittiva.it

¹⁶ www.intelligenzaartificialeegiustiziadelgiudice.it

¹⁷ L. VIOLA, *Giustizia predittiva e interpretazione della legge con modelli matematici*, Roma, 2018. Da una parte c'è la spinta a fare di più e meglio, dall'altra c'è l'obiettivo di aggiornare le strutture dello studio all'evoluzione in corso. Anche nella relazione con il cliente la disintermediazione è la regola. Parte dello sforzo di progettazione risiede

capacità di calcolare la probabilità di un esito giudiziario sulla base di un algoritmo o a base statistica oppure, vedremo, a base logica. In modo più semplice, i sistemi di giustizia predittiva sono destinati a essere utilizzati da parte di uffici legali, assicuratori (sia per le loro esigenze interne che per i loro assicurati), nonché avvocati, al fine di anticipare l'esito di una controversia. Teoricamente potrebbero anche aiutare i giudici a prendere delle decisioni. Un esempio di quando è stata utilizzata la tecnologia in ambito giudiziario, risale allo scorso 14 agosto 2018, data che segna la caduta del ponte Morandi a Genova¹⁸. Qui, la Procura di Genova ha deciso di utilizzare un software dell'FBI¹⁹, dotato di algoritmi particolarmente complessi, con l'obiettivo di incrociare tutti i dati raccolti con quelli dei dispositivi elettronici sequestrati, con la documentazione tecnica ed i pareri dei consulenti sia del P.M. che della difesa. Mentre qui tutto ciò può sembrare ai nostri occhi una novità, in altri stati già da tempo utilizzano software ai fini giudiziari. Basti pensare al sito "ROSS Intelligence" che, munito di un ricco database di giurisprudenza, consente agli avvocati di redigere atti tenendo conto dell'orientamento dei giudici su un determinato argomento. Chi ce lo dice che in un futuro giudici e avvocati non utilizzeranno sistemi in grado di ridurre il tempo, le ore di lavoro e aumentare la precisione? Chi ce lo dice che in questo campo l'utilizzo della tecnologia può solo rilasciare aspetti negativi? Perché non potremmo pensare un domani ad un giudice dietro un computer? La ricerca più affascinante è stata fatta presso lo University College London (UCL, Londra, UK). Qui i ricercatori hanno creato un giudice virtuale, e gli hanno sottoposto diversi casi che sono stati trattati dalla Corte Europea per i diritti Umani. Il risultato è che nel 79% dei casi il computer ha emesso lo stesso verdetto dei giudici in carne e ossa. La differenza del 20% è da attribuire a quei casi in cui la corte ha interpretato le leggi invece di applicarle alla lettera; situazioni in cui si può affermare che i giudici sono più realisti che formalisti. Anche questa teoria è stato oggetto di dibattito e lunghe discussioni e lo è ancora tutt'oggi, perché per chi come i sostenitori della scuola Perlingieriana, il giudice²⁰ non deve applicare la legge così com'è, deve infatti confrontarsi con diversi istituti e dalla combinazione di questi ultimi prendere una decisione. Sempre secondo i sostenitori della scuola di Perlingieri, il giudice non può ai fini dell'emanazione di un provvedimento tenere solo un'interpre-

nell'obiettivo di sollevare gli studi legali dalle attività di commodities e nel supportare i clienti nell'attività di business intelligence.

¹⁸ www.corrieredellasera.it

¹⁹ www.intelligenzaartificialeegiustiziadelgiudice.it

²⁰ G. PERLINGIERI, *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015.

tazione assiologica, ma anche funzionale e sistematica. Il diritto va sempre storicizzato, cioè va rapportato al contesto storico in cui ci troviamo. Pensiamo ad esempio al concetto di buona fede²¹; questo veniva utilizzato ai tempi del fascismo, ai tempi del codice del 1865 e nel codice de 1942.

Ma può un computer anticipare il ragionamento giuridico? La modellizzazione informatica del ragionamento dei giudici²² si è dimostrata altrettanto impossibile di quella dei sistemi giuridici positivi. Come sottolineato dalla dottrina, il ragionamento del giudice è soprattutto una questione di valutazione e interpretazione dei fatti dimostrati e pertinenti a una causa e delle norme di diritto applicabili (presenti nei testi o nei precedenti), il cui significato, come si è detto, resta indeterminato nonché di interpretazione soggettiva del concetto di equità, che in Europa dovrebbe subire nuove modifiche per via dell'esigenza, incoraggiata dalla Corte europea dei diritti dell'uomo, di un controllo di proporzionalità. La complessità del diritto è costituita dalla sua natura teleologica e contentuosa: due rilievi coerenti possono condurre a sentenze diverse in funzione di due diverse priorità. Ciò accade perché il famoso sillogismo giuridico è più una maniera di presentare il ragionamento giuridico che non la sua traduzione formale. Non rispecchia per intero il ragionamento del giudice, che è composto in realtà da una moltitudine di fattori decisionali, non può essere formalizzato a priori, ed è talvolta fondato sul suo potere discrezionale: quali sono i fatti pertinenti? Tali fatti sono accertati? Quali norme si applicano a essi? Quale è il significato di tale norma in relazione alla causa da decidere? Quale fonte deve prevalere in una pluralità di fonti confliggenti? La complessiva coerenza delle decisioni giudiziarie non si realizza mai, si tratta più di una descrizione a posteriori utilizzata dai giudici nelle motivazioni, intesa più a convincere loro stessi della validità di una soluzione specifica che a descrivere in maniera rigorosa e oggettiva tutte le fasi che hanno condotto alla decisione adottata. I risultati cui pervengono le intelligenze artificiali sono in realtà indipendenti dalla questione della conformità al diritto di una particolare soluzione e non sono in grado di distinguere le argomentazioni legittime da quelle illegittime (come farebbe in realtà un giudice in qualità di persona fisica).

In effetti il giudice, nel momento dell'applicazione della norma, utilizza fondamentalmente due tipi di ragionamento: uno volto ad individuare le premesse normative (le norme pertinenti), l'altro volto a ricavare la soluzione normativa, date le premesse. La prima fase ha a che fare con gli

²¹ Art. 1175 c.c., «Il creditore e il debitore devono comportarsi secondo buona fede».

²² www.ilcatalogodeigiuristi.it

aspetti fattuali, cioè con le particolarità che il caso individuale presenta rispetto al dettato necessariamente generale ed astratto della norma: il giudice, che dovrà individuare la norma da cui ricavare la conclusione, esaminerà la fattispecie, intesa come una collezione di fatti; eliminerà i fatti irrilevanti e quindi classificherà i fatti rilevanti secondo un determinato ordine o criterio, cercando poi di trasferirli ad un livello più generale che consenta un confronto con gli enunciati normativi. Sembrerebbe che tali operazioni siano completamente prive di regole logiche, in quanto basate sull'analisi dell'uso linguistico delle parole: in realtà è possibile individuare, alla base, uno schema di ragionamento logico riconducibile all'induzione. Difatti, dopo l'accertamento dei fatti il giudice è in grado di individuare le premesse normative da applicare: negli ordinamenti a civil law le premesse saranno in massima parte da ricercarsi nelle leggi, negli ordinamenti a common law nei precedenti.

Inoltre l'esigenza di riconoscere caratteristiche strutturali proprie di sottosistemi giuridici assume particolare rilevanza nel momento interpretativo ove si riscontri l'insufficienza dei tradizionali principi sistematici nella risoluzione dei conflitti fra norme; a livello di descrizione di un sistema giuridico, che è quella che bisogna prendere in considerazione, è sufficiente disporre di parametri per la definizione di un sottosistema e di criteri organizzativi omogenei per strutturarlo.

È in tale ottica che assume rilevanza la giustizia predittiva che dopo aver ricondotto le diverse forme di interpretazione a modelli matematici, passa alla concreta applicazione della propria teoria analizzando specifiche sentenze fino ad ipotizzare la realizzazione di una vera e propria giustizia predittiva. Ma allora ciò cosa potrebbe comportare: ridurre la decisione di un giudice all'applicazione di una formula matematica? Magari fino ad arrivare allo scenario prospettato da Jacques Charpentier nella sua opera *Justice machines* dove l'applicazione della giustizia viene affidata ad apparecchi cibernetici?

Come giustamente sostiene Jonas bisogna evitare che «sviluppi tecnologici di volta in volta avviati con obiettivi a breve termine, presentino la tendenza a rendersi autonomi acquisendo una propria dinamica coattiva in forza della quale non solo diventano irreversibili, ma acquistano una funzione propulsiva al punto da trascendere la volontà ed i piani degli attori»²³.

²³ H. JONAS, *Il principio di responsabilità*, Torino, 1979.

4. Privacy e sicurezza

Le applicazioni di intelligenza artificiale sono state oggetto di particolare attenzione da parte del legislatore comunitario che nel regolamento europeo n. 2016/679 all'art. 22 ribadisce come principio generale che l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida allo stesso modo significativamente sulla sua persona.

Tale disposizione non si applica quando la decisione:

a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, oppure

b) sia autorizzata dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato, oppure

c) si basi sul consenso esplicito dell'interessato.

Non bisogna mai dimenticare che le nozioni di *digital footprint*, identità e profilazione degli utenti in internet, sono concetti tra loro strettamente collegati.

Il termine *digital footprint*, viene comunemente utilizzato per indicare le tracce di dati che vengono disperse nella rete a seguito di determinate interazioni avvenute all'interno dell'ambiente digitale, questi dati contengono usualmente informazioni riguardanti le diverse interazioni che un soggetto può eseguire in un contesto digitale. Questi dati ed informazioni possono concorrere nel formare anche una identità digitale.

A tal fine è possibile individuare almeno due tipi di informazioni che possono essere reperite on-line e riguardanti un soggetto determinato, un primo tipo, che potremmo definire di *informazioni primarie* e riguardanti i caratteri personalissimi dell'individuo, ed altri tipi di *informazioni secondarie*, riguardanti le abitudini sociali ed i gusti commerciali dell'utente interessato, questi due tipi di informazioni, elaborate tra loro, formano il cd. profilo-utente.

Da queste brevi premesse, si pongono alla nostra attenzione una serie di questioni, occorre anzitutto domandarsi quali siano gli interessi che sottostanno ad una operazione di profilazione e in seconda analisi quali tutele sono esperibili in tali situazioni.

Come noto, la maggior parte dei moderni dispositivi di comunicazione, al momento del loro utilizzo attraverso il collegamento ad Internet, frammentano e disperdono delle tracce che provano

l'utilizzo del dispositivo e la contestuale presenza dell'utente in rete. Nella pratica il problema della profilazione e della dispersione dei dati personali, si manifesta in modo particolare nei momenti della navigazione in internet mediante browser (si pensi ai cookies) e nell'utilizzo delle più comuni piattaforme di social networking come strumenti relazionali e di comunicazione.

A tal fine vengono sempre più utilizzate anche tecniche di reperimento di informazioni utili al ciclo di intelligence tramite il monitoraggio e l'analisi dei contenuti scambiati attraverso i Social Media come la SOCIAL Media INTelligence (SOCMINT).

L'obiettivo principale della profilazione è la pubblicità comportamentale, che pensata e cresciuta nel mondo delle comunicazioni informatiche, prevede il tracciamento delle informazioni rilasciate dagli utenti durante la navigazione in internet, al fine di creare segmenti pubblicitari *ad personam*, modellati sugli interessi dell'utente considerato. Tale attività di per sé non è illecita o vietata, ma con il crescente bisogno di proteggere le identità digitali e i dati sensibili degli utenti, negli ultimi anni l'Unione europea si è mossa in maniera molto decisa verso la creazione di direttive e linee guida contenenti discipline di regolamentazione nelle comunicazioni elettroniche e di protezione dei dati nonché delle informazioni riguardanti gli utenti di internet, per dare ai naviganti strumenti attraverso i quali poter essere sempre al corrente dell'eventuale monitoraggio che può avvenire sulle loro tracce digitali.

Il recente Regolamento europeo n. 2016/679 in realtà ha un occhio particolare per tali attività che vengono considerate degne della massima attenzione in quanto spesso connesse ad evolute tecniche di intelligenza artificiale.

Si pensi a quanto disposto dall'art. 4 del GDPR che definisce la profilazione «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica».

La stessa preoccupazione del legislatore è evidente quando al considerando 71 specifica che «al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare,

che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori».

Il Gruppo di Lavoro ex articolo 29 dei Garanti Privacy europei ha pubblicato il 3 ottobre 2017 le Linee Guida in tema di processo decisionale automatizzato e profilazione rispetto alle regole enunciate dal Regolamento europeo 2016/679 - GDPR.

Queste Linee Guida, così come altre recentemente adottate (in tema di responsabili della protezione dei dati, portabilità dei dati e valutazione d'impatto sulla protezione dei dati), hanno lo scopo di chiarire meglio le disposizioni del GDPR su specifici argomenti, riportando anche esempi e casi pratici offerti dall'esperienza acquisita negli Stati membri.

Il ricorso a processi decisionali automatizzati, compresa la profilazione automatizzata, si sta viepiù diffondendo in diversi settori, sia privati che pubblici, perché il progresso tecnologico ha reso questi trattamenti maggiormente efficienti ed economici.

A riguardo, tuttavia, il GDPR ravvisa possibili rischi significativi per i diritti e le libertà degli individui riconnessi a:

- la tendenziale opacità dei processi e meccanismi automatizzati che porta spesso l'individuo, oggetto di profilazione, a non esserne a conoscenza;

- la creazione, da parte del titolare, di dati nuovi, aggiuntivi rispetto agli originali che potrebbero "incoltare" l'interessato in una categoria a cui non si riconosce condizionando così le sue scelte e, in alcuni casi, portando anche a forme di discriminazione.

Pertanto, il GDPR, per correggere questo dislivello informativo tra titolare e interessato ed evitare pregiudizi alla sfera giuridica di quest'ultimo, individua una serie di requisiti su cui concentrarsi per rendere questi trattamenti automatizzati conformi alla normativa:

- specifiche prescrizioni in tema di trasparenza e correttezza;
- maggiori obblighi di accountability;
- basi giuridiche specifiche per la legittimazione del trattamento;
- garanzie per gli individui in tema di diritto di opposizione alla profilazione e, in particolare, alla profilazione per finalità di marketing;
- esecuzione di una valutazione d'impatto sulla protezione dei dati laddove non siano soddisfatte certe condizioni.

Ma ultimamente stanno assumendo in rete notevole diffusione altri sistemi di IA come i c.d. chatbot (dal termine più generale bot, diminutivo di robot). Con tale termine si intende un software basato sull'Intelligenza Artificiale, in grado di simulare una conversazione intelligente con l'utente su una chat. Di fatto offre un servizio funzionale e di supporto attraverso le principali piattaforme di messaggistica come Slack, Telegram, Facebook Messenger. Può essere utilizzato in diversi settori: customer care, diffusione di notizie, offerte e promozioni, e-commerce, attivazione di servizi. Il software si contraddistingue per essere autonomo e sempre attivo per offrire agli utenti aiuto e risposte, ma nello stesso tempo tracciarne interessi, preferenze, età e gusti ai fini marketing e pubblicità comportamentale.

Ovviamente anche questi sistemi vanno continuamente monitorati per le evidenti implicazioni che possono comportare in materia di privacy.

Proprio per la notevole rilevanza assunta negli ultimi tempi dall'IA in vari settori della nostra società il 21 marzo 2018 è stato presentato a Roma il primo Libro Bianco *L'Intelligenza Artificiale a servizio del cittadino* a cura della task force IA dell'Agenzia per l'Italia digitale.

Il Libro Bianco illustra le linee guida e le raccomandazioni per l'utilizzo sostenibile e responsabile dell'Intelligenza Artificiale nella Pubblica amministrazione e rappresenta l'inizio di un percorso progettuale: per questo sono stati destinati 5 milioni di euro allo sviluppo di progetti pilota di Intelligenza Artificiale per le amministrazioni che collaboreranno con l'Agenzia all'individuazione delle iniziative.

I progetti potranno riguardare diversi ambiti d'applicazione individuati dal Libro Bianco. Tra questi: i chatbot, i sistemi automatici di diagnostica in grado di individuare velocemente la patologia di un paziente, le piattaforme automatiche per supportare gli insegnanti nella valutazione dei compiti scolastici, i sistemi avanzati di elaborazione dei dati per contrastare l'evasione fiscale e altro ancora.

Ad ogni modo di fronte al sempre maggiore utilizzo di complessi sistemi di IA appare evidente l'importanza dell'approccio tipico della privacy by design disciplinata dall'art. 25 del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016.

Il principio della privacy by design richiede che la tutela dei diritti e delle libertà degli interessati con riguardo al trattamento dei dati personali comporti l'attuazione di adeguate misure tecniche e organizzative al momento sia della progettazione che dell'esecuzione del trattamento stesso, onde garantire il rispetto delle disposizioni del Regolamento UE 2016/679.

La privacy by design può essere definita la nuova dimensione della privacy che trae le sue origini dall'innovazione tecnologica e dal progresso delle comunicazioni elettroniche.

L'evoluzione, quindi, tocca anche il settore della privacy rispetto alla tradizionale e primaria configurazione con il riferimento alle PET (acronimo di Privacy Enhancing Technologies) che costituiscono le tecnologie utilizzate per migliorare il diritto alla privacy. Ovviamente tali tecnologie vengono considerate in maniera neutra, ovvero senza alcuna connessione con specifiche fattispecie. Tale espressione fu utilizzata per la prima volta nel report pubblicato nel 1995 dal titolo *Privacy-enhancing technologies: the path to anonymity*, della Data Protection Authority olandese in collaborazione con il Commissario dell'Ontario (Canada).

Il concetto di Privacy by Design trova spazio nella trilogia di applicazioni: 1) IT systems; 2) accountable business practices; and 3) physical design and infrastructure. In sostanza:

- 1) Tecnologia dell'informazione;
- 2) Pratiche commerciali responsabili;
- 3) Progettazione delle strutture.

Al fine di garantire e dimostrare la conformità con il Regolamento, il titolare del trattamento deve adottare politiche interne e attuare misure adeguate, che soddisfino in particolare i principi della privacy by design e della privacy by default.

Il principio della privacy by design prevede che la protezione dei dati sia integrata nell'intero ciclo di vita della tecnologia, dalla primissima fase di progettazione fino alla sua ultima distribuzione, all'utilizzo e all'eliminazione finale.

Il principio della privacy by default prevede che le impostazioni di tutela della vita privata relative ai servizi e prodotti rispettino i principi generali della protezione dei dati, quali la minimizzazione dei dati e la limitazione delle finalità.

Con questa nuova concezione della privacy si è così maggiormente diffusa l'esigenza di assicurare una forte tutela dei diritti e delle libertà delle persone, con particolare riferimento all'identità personale e alla vita privata degli individui che utilizzano le reti telematiche.

MICHELE IASELLI
Università degli Studi di Cassino
e del Lazio Meridionale