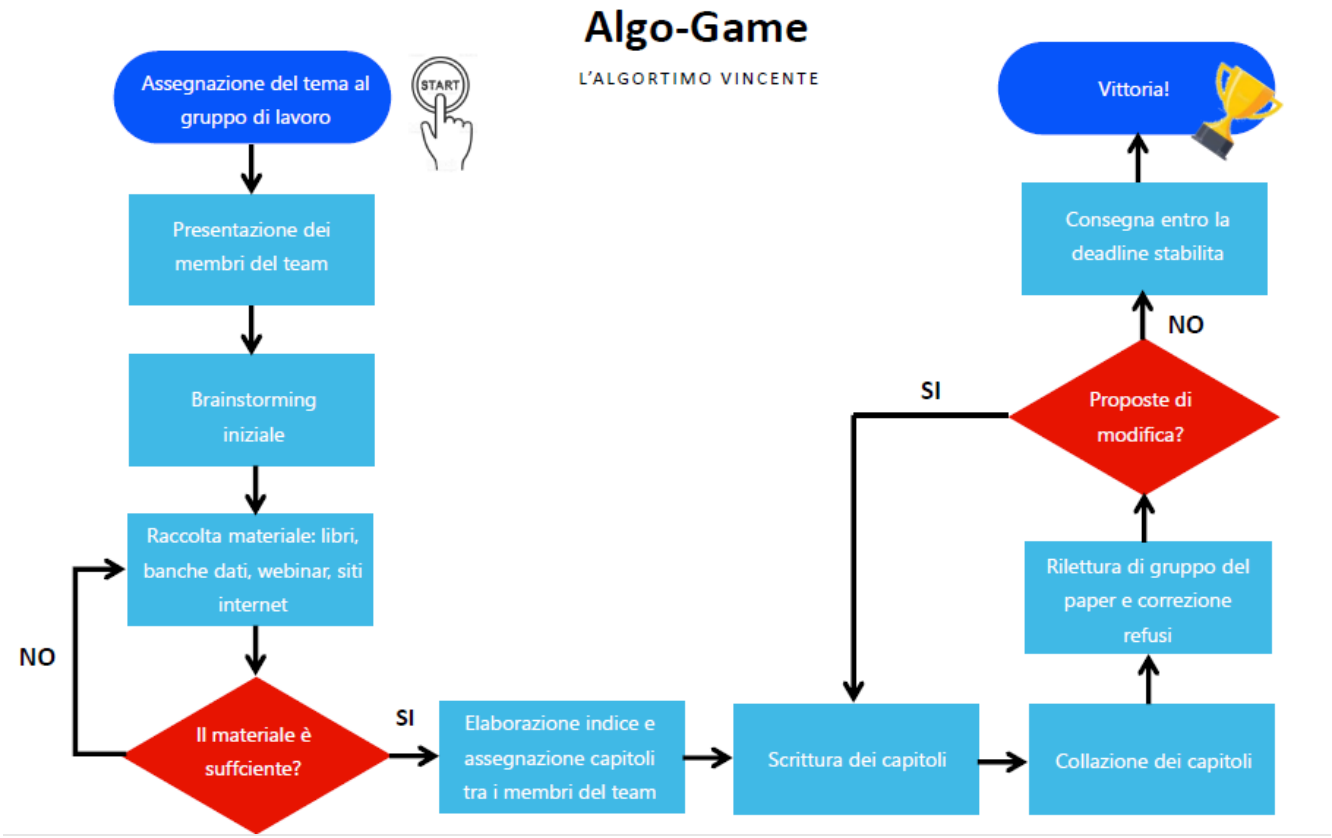
Intelligenza artificiale, algoritmi e IP

Analisi dei correlati aspetti giuridici ed etici

https://www.quotidianogiuridico.it/documents/2021/06/03/regolamento-ue-sull-intelligenza-artificiale-uno-strumento-articolato-per-gestire-il-rischio

---

Tutto è iniziato da un algoritmo ...il nostro Algo-Game!

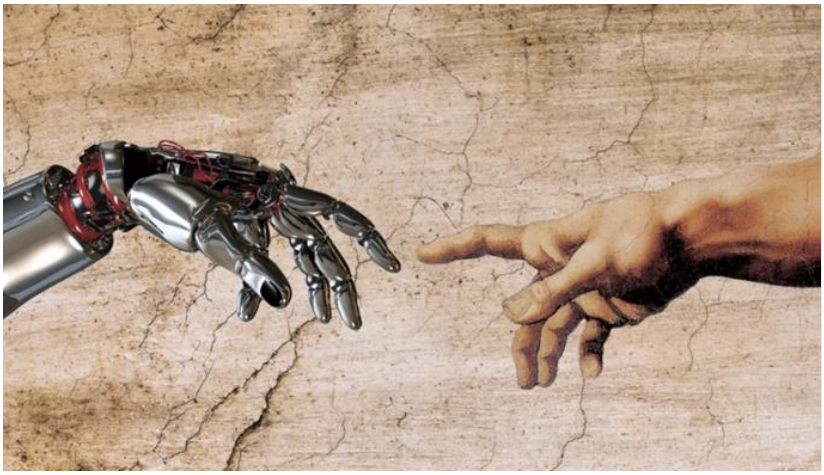


Il Gruppo di lavoro

Fabrizia Cicero
Elisa D'Amico
Laura Fragapane
Adele Necchia
Federica Saraceni
Sabrina Panfili (tutor)

Indice

Executive Summary



https://www.industriaitaliana.it/nei-processi-decisionali-basati-su-ai-la-fiducia-e-estremamente-importate/

In a context of quick technological changes, the evolution from the concept of algorithm, starting from the software one to the artificial intelligence (that we will call "AI"), it happened in a very natural way and it invaded our lives, without us knowing realizing it and in a more and more easily way, without any particular instruction. Newborns perfectly use naturally instruments whose operation is based on artificial intelligence. This progress cannot be interrupted, but without ever loose sight human respect and his fundamental rights, hence the need for a necessary balance between innovation and legal protection of human rights.

The topics covered in this paper are wide, complex and fascinating, but at the same time disturbing. Starting from the analysis of the algorithms, which based on mathematical formulas, don't have any legal protection, we saw how those same became the object of an important legal protection when they find practical application through the software. So, we mastered different types of software protection, both at national and EU level, noticing how these different forms of protection now make it possible to undoubtedly reach a high level of protection with compared to its authors and producers.

These certainties are lost when the software is examined by the AI systems. Systems that, although based on software, exploit predictive models which, through the processing of huge amounts of data

and information, are able to develop reasoning and results capable of replacing human reasoning and making decisions in place of man. The potential application of AI-based technologies knows no bounds: they are now rooted in some strategic commercial sectors and are already entering into others, very delicate ones, such as medical-health, economic-financial and even legal. The possible obstacles to their dissemination will certainly not be of a technological nature but rather of an ethical nature and only adequate legal protection can guarantee the right balance between technological development and protection of fundamental human rights.

We have therefore examined specifically the models of "machine learning" and "deep learning", systems which, on the one hand, will improve the quality of life, on the other, evolve in such a complex way that man himself is not able to rule all the way. In this context, it is therefore essential to guarantee every human being the ability to fully and safely exploit the advantages deriving from AI-based technologies, and this can only happen if the processes upstream prove to be reliable.

The European Union has for some time been moving in this direction. On April 21, the European Commission published a proposal for a Regulation that lays the foundations for addressing the risks associated with the use of artificial intelligence. The proposal follows an approach devoted to ethics and the concept of the search for trust in new technologies and represents a further piece in the mosaic of technological-legal regulations already issued by the EU, which also includes the "Ethical guidelines finals for reliable artificial intelligence ", made public on 8 April 2019, which collect the guidelines of an independent group of high-level experts on artificial intelligence, established by the European Commission in June 2018; the conclusions can be summarized as follows: in order for AI systems to be reliable they must have three essential characteristics: legality, ethics and robustness.

Eventually we dealt with the topic of the intellectual property of AI: who is the author and the owner of the patent in the case of inventions made by AI? Who is entitled to the copyright for intellectual creations made by AI? Also on this front, the AI is opening up scenarios and asking completely new questions that cannot be framed in the current regulatory framework and about which the academic world is questioning itself. The European Patent Office rejected two patent applications in which an AI system was designated as inventor, on the basis that, according to Art. 81 and of Rule 19 of the European Patent Convention, the inventor must be an individual.

Identifying an artificial intelligence system as an "inventor" would essentially require not only that we accept the fact that an AI system can be equated with individuals, but also full recognition of legal rights to AI algorithms. Even if today, most of the countries around the world share the position of the European Patent Office, in the next few years some of our "legal certainties" could waver to give an answer to technological evolution and who knows that, after the "physical" and "legal" personalities, a "digital" personality will not be introduced?

* * *

In un contesto di rapidi cambiamenti tecnologici, l'evoluzione dal concetto di algoritmo, da quello di software e fino a quello di Intelligenza Artificiale (che di seguito chiameremo "AI") è avvenuta in maniera del tutto naturale ed ha pervaso le nostre vite, senza che noi ce ne rendessimo conto ed in maniera sempre più facile, senza bisogno di particolari istruzioni. I bambini a pochi anni dalla nascita usano perfettamente e con naturalezza strumenti il cui funzionamento è basato sull'intelligenza artificiale. Questo è il progresso e non può certo essere interrotto, ma senza perdere di vista il rispetto per l'uomo e per i suoi diritti fondamentali, da qui l'esigenza di un necessario bilanciamento tra innovazione e tutela giuridica dei diritti dell'uomo.

I temi affrontati in questo elaborato sono ampi, complessi e affascinanti, ma al tempo stesso inquietanti. Partendo dall'esame degli algoritmi, che alla stregua di formule matematiche, non godono di per sé di una specifica protezione giuridica, abbiamo visto come gli stessi diventano invece oggetto di rilevante tutela giuridica nel momento in cui trovano applicazione pratica attraverso il software.

Abbiamo quindi approfondito i diversi tipi di tutela oggi riservata al software, tanto a livello nazionale quanto a livello comunitario, rilevando come tali diverse forme di tutela consentano ormai di raggiungere indubbiamente un alto livello di protezione rispetto ai propri autori e produttori.

Tali certezze vengono meno quando dal software si passa all'esame dei sistemi di AI. Sistemi che, ancorché basati sul software, sfruttano modelli predittivi che, attraverso l'elaborazione di enormi

quantitativi di dati ed informazioni, arrivano a sviluppare ragionamenti e risultati in grado di sostituire il ragionamento umano e prendere decisioni al posto dell'uomo.

La potenziale applicazione delle tecnologie basate sull'AI non conosce limiti: sono ormai radicate in alcuni settori commerciali strategici e stanno già inserendosi in altri, anche molto delicati, come quello medico-sanitario, economico-finanziario e perfino giuridico.

I possibili ostacoli alla loro diffusione non saranno certo di natura tecnologica ma piuttosto di natura etica e solo una tutela giuridica adeguata potrà garantire il giusto bilanciamento tra sviluppo tecnologico e tutela dei diritti fondamentali dell'uomo.

Abbiamo quindi esaminato nello specifico i modelli di "machine learning" e di "deep learning", sistemi che se da un lato saranno in grado di migliorare la qualità della vita, dall'altro si evolveranno in modo così repentino e complesso che l'uomo stesso potrebbe non essere in grado di governarli fino in fondo.

In tale scenario, diventerà quindi fondamentale garantire ad ogni essere umano la possibilità di sfruttare pienamente e con sicurezza i vantaggi derivanti dalle tecnologie basate sull'AI, ma ciò potrà avvenire solo se i processi posti a monte si riveleranno assolutamente affidabili.

L'Unione Europea da tempo si sta muovendo in tal senso. Lo scorso 21 Aprile, la Commissione Europea ha pubblicato una proposta di Regolamento che pone le basi per affrontare i rischi associati all'utilizzo dell'intelligenza artificiale. La proposta segue un approccio votato all'etica e al concetto di ricerca della fiducia nelle nuove tecnologie e rappresenta un ulteriore tassello nel mosaico di norme tecnologico-giuridiche già emanate dell'UE, all'interno del quale si collocano anche le "*Linee guida etiche finali per un'intelligenza artificiale affidabile"*, rese pubbliche l'8 Aprile 2019, che raccolgono gli orientamenti di un gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale, istituito dalla Commissione Europea nel giugno 2018; le conclusioni sono così sintetizzabili: perché i sistemi di AI siano affidabili devono avere tre caratteristiche essenziali: legalità, eticità e robustezza.

Abbiamo infine affrontato il tema della proprietà intellettuale dell'AI: chi è l'autore ed il titolare di brevetto nel caso di invenzioni realizzate da AI? A chi spettano i diritti patrimoniali d'autore per creazioni intellettuali realizzate da AI? Anche su questo versante l'AI sta aprendo diversi scenari e ponendo interrogativi completamente nuovi, rispetto ai quali il mondo accademico si sta interrogando.

L’Ufficio Europeo dei brevetti ha rifiutato due domande di brevetto in cui veniva designato, come inventore un sistema di AI, in quanto , secondo l’Art. 81 e della Regola 19 della Convenzione Europea dei Brevetti, l’inventore deve essere una persona fisica.

Identificare un sistema di intelligenza artificiale come “inventore” richiederebbe, quindi l’equiparazione di un sistema di AI alle persone fisiche o giuridiche, con il pieno riconoscimento di diritti di natura legale ad un sistema di algoritmi .

Anche se ad oggi, la maggior parte dei Paesi di tutto il mondo condivide la posizione dell’Ufficio Europeo dei brevetti, nei prossimi anni alcune delle nostre “certezze legali” potrebbero vacillare e chissà che, di fronte all’avanzare dell’evoluzione tecnologica, non si arrivi ad introdurre nuove forme di personalità …., dopo la personalità “fisica” e quella “giuridica”, avremo anche una personalità “digitale”?

CAPITOLO 1 - ALGORITMI E SOFTWARE *a cura di Adele Necchia*

https://www.cibiexpo.it/gli-algoritmi/

1.1 Definizione di algoritmo

Il termine "algoritmo" deriva dalla trascrizione latina del nome del matematico arabo Mohammad ibn-Musa al-Khwarizmi, così chiamato perché nativo della regione dell'Asia Centrale del Khwarezm (l'antica Coresmia, località che fa parte dell'odierno Uzbekistan).

Questo matematico, che visse tra il 780 e l'850 d.c., fu studioso presso la *Bayt al-Ḥikma*, la Casa della sapienza, voluta dal califfo Al-Maʾmun, dove ebbe modo di dedicarsi alle ricerche, alla traduzione di manoscritti scientifici greco-ellenistici e alla stesura delle proprie opere. In particolare, il trattato sull'algebra *Hisab al-Jabr*.

Per algoritmo si intende qualunque schema o procedimento sistematico di calcolo che permette la risoluzione di un problema specifico attraverso l'applicazione, in un determinato ordine, di una serie finita di istruzioni.

Da questa definizione si deducono quindi le caratteristiche fondamentali che qualunque algoritmo deve avere:

a) le istruzioni che costituiscono l'algoritmo devono essere elementari, ovvero non ulteriormente divisibili (atomicità);

b) le istruzioni che costituiscono l'algoritmo devono essere interpretabili in modo diretto ed univoco dall'esecutore, sia esso umano o artificiale (non ambiguità);
c) l'algoritmo deve essere finito, ossia composto da un numero definito di istruzioni e deve presentare un punto di inizio dove comincia il procedimento risolutivo e un punto di fine, raggiunto il quale si interrompe l'esecuzione delle istruzioni (finitezza);
d) l'esecuzione dell'algoritmo deve avvenire entro un tempo finito (terminazione);
e) l'esecuzione dell'algoritmo deve condurre ad un unico risultato (effettività);
f) ogni esecuzione successiva dell'algoritmo sugli stessi dati di input devono produrre sempre lo stesso risultato finale (riproducibilità).

In sintesi, possiamo definire l'algoritmo come una sequenza finita di passi necessari per risolvere un problema o raggiungere un determinato obiettivo. Il programma invece è la traduzione dell'algoritmo in un linguaggio di programmazione comprensibile per il computer. Il diagramma di flusso è la notazione grafica usata per descrivere in modo intuitivo le azioni di cui è fatto un algoritmo. L'insieme di tutti i programmi che consentono un'efficiente utilizzazione delle risorse del calcolatore elettronico s'indica genericamente con il termine inglese "software". Ad oggi i termini software e programma sono usati in modo intercambiabile poiché spesso si riferiscono alla stessa cosa nell'uso quotidiano.

1.2 Definizione di software

Il termine software inteso come istruzioni impartite ad un computer viene usato per la prima volta nel 1958 dallo statistico americano John Wilder Turkey.

Il termine "software" è composto dalle parole inglesi "soft" (morbido) e "ware" ("componente") ed indica infatti tutte le componenti "leggere", non materiali di un computer e, più in generale, di un dispositivo elettronico.

Si distingue dall'hardware che invece identifica le componenti fisiche "pesanti" del computer, cioè tutti gli elementi fisici: meccanici, elettrici, elettronici e ottici che lo compongono, inclusi stampanti, schermo e tastiere.

Il software è quindi un programma per elaboratore sviluppato tramite un linguaggio di programmazione. È composto da una sequenza di istruzioni logiche che permettono al computer di compiere operazioni utili per l'utente finale.

Prendendo in considerazione il grado di utilizzabilità e prossimità rispetto all'utente, i software si distinguono principalmente in:

a) software di base o sistemi operativi: si tratta di software indispensabili in quanto permettono e gestiscono il funzionamento di tutte le risorse hardware del computer. Esempi di sistemi operativi sono Windows, Linux, Android, iOS, DOS, etc. Essi sono progettati per fornire una piattaforma di appoggio per gli altri software. Grazie a tali tipi di software possiamo eseguire le operazioni più comuni, ad esempio quando premiamo un tasto sulla tastiera, il computer sa che deve far comparire sul monitor la relativa lettera. Oppure ogni volta in cui con il mouse pigiamo su un dato programma, grazie al sistema operativo, quel dato programma sarà avviato.
b) software dell'utente o software applicativi: si tratta di un programma o un insieme di programmi (suite) sviluppati per risolvere un problema specifico dell'utente finale. Per funzionare, richiedono la presenza del sistema operativo. Esempi di software applicativo sono programmi come Word, Excel, PowerPoint, Google Chrome, Internet Explorer, etc. Tali tipologie di software, proprio perché sono idonei ad esercitare una funzione per l'utente finale, trasformano il computer in una macchina per svolgere un compito specifico.

In conclusione, per software si intende il complesso di tutte le istruzioni necessarie a far eseguire al computer un determinato lavoro.

Un'altra definizione di software di matrice internazionale è stata coniata dall'Organizzazione Mondiale della Proprietà Intellettuale (OMPI) nel 1984 in base alla quale viene definito come: "espressione di un insieme organizzato e strutturato di istruzioni (o simboli) contenuti in qualsiasi forma o supporto (nastro, disco, film, circuito), capace direttamente o indirettamente, di far eseguire o far ottenere una funzione, un compito od un risultato particolare per mezzo di un sistema di elaborazione elettronica dell'informazione". Quest'ultima è quella più completa maggiormente condivisa in campo internazionale, che si presta meglio per definire l'esatto inquadramento giuridico del software.

Da queste definizioni deriva l'appartenenza del software ai beni giuridici immateriali, e in particolare alla categoria delle creazioni intellettuali.

Il software viene creato da tecnici specializzati, detti programmatori o sviluppatori o developers, che ne definiscono il codice sorgente (o sorgente o anche listato), utilizzando appositi linguaggi di programmazione, tra i principali C, C #, C ++, C #, Java e Python.

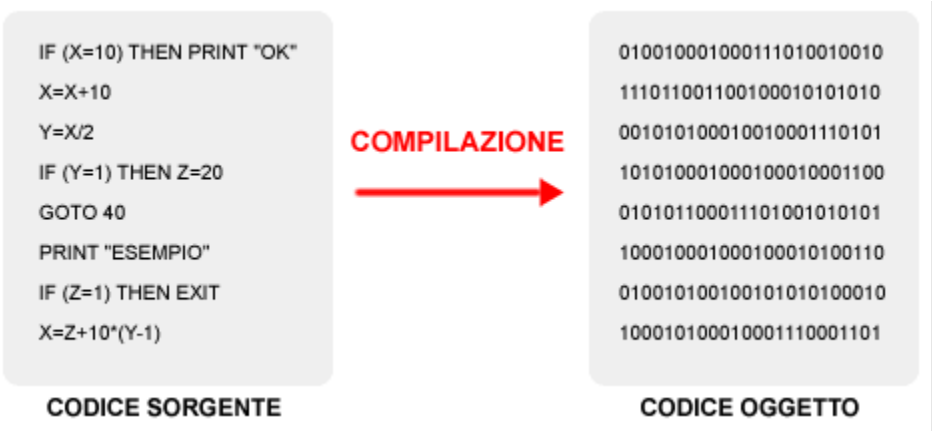
Quindi, in sostanza, il codice sorgente è la raccolta di istruzioni che, utilizzando un determinato linguaggio di programmazione, definiscono le funzionalità del software richiesto.

Di seguito viene mostrato un esempio di codice sorgente molto semplice che se compilato con un compilatore C, crea un file di tipo .exe che mostra la scritta “Ciao mondo!” [1].

```
#include <stdio.h>
#include <stdin.h>
int main(void)
{
printf(“Ciao mondo! \n”);
return 0;
}
```

Si utilizzano i linguaggi di programmazione perché è sicuramente più facile per l’uomo programmare il software in un linguaggio simile a quello naturale piuttosto che in linguaggio binario o esadecimale.

Affinché un software sia eseguito da un computer, il codice sorgente deve essere preliminarmente tradotto in altra forma c.d. “codice oggetto”.



Siffatta operazione per cui il codice sorgente (comprensibile per l’uomo) viene tradotto in codice oggetto (un linguaggio comprensibile solo per l’elaboratore) è denominata “compilazione”.

[1] Da: https://vitolavecchia.altervista.org/che-cose-il-codice-sorgente-in-informatica/

La trasformazione da codice sorgente a codice oggetto è svolta dai programmatori attraverso l'utilizzo di appositi software denominati appunto compilatori. In questo modo, il software diventa eseguibile dal computer[2].

La compilazione, quindi, crea l'oggetto eseguibile (es. file .exe) dal sistema operativo che sarà utilizzato dagli utenti finali.

Tale trasformazione è unidirezionale: una volta eseguita, non consente più di risalire dal codice oggetto al codice sorgente. L'utente finale non può modificare l'oggetto, né può leggere il file sorgente del programma. Soltanto lo sviluppatore del software può apportare modifiche al programma.

Per effettuare il processo inverso, ovvero ricostruire il codice sorgente partendo dal codice oggetto, è necessario implementare un'altra operazione, la c.d. "decompilazione" (o in inglese "reverse engineering").

Anche per tale tipo di operazione, sono utilizzati specifici tool informatici. Tuttavia, affinché l'attività di decompilazione sia lecita, devono sussistere determinate condizioni:

a) deve essere eseguita dal licenziatario o da altri che abbia il diritto di usare una copia del programma, oppure, per loro conto, da chi è autorizzato a tal fine;
b) le informazioni per conseguire interoperabilità non devono essere già facilmente e rapidamente accessibili;
c) deve essere limitata alle sole parti del programma originale necessarie per conseguire l'interoperabilità[3].

Generalmente è molto difficile che il proprietario renda disponibile il codice sorgente del proprio programma. Infatti, una volta che si dispone del codice sorgente sarà possibile per l'utente correggere e modificare il programma, ma anche, compresone il funzionamento, di copiarlo con relativa facilità.

Proprio per questo, nei modelli contrattuali generalmente utilizzati per la concessione in uso del programma, il proprietario quasi sempre si riserva ogni facoltà di accesso al codice sorgente vietando l'attività di decompilazione[4].

[2] Da: https://www.andreaminini.com/informatica/software/
[3] M.G. Jori, Diritto Nuove Tecnologie e Comunicazione Digitale, p. 4.
[4] C. Rossello, I Contratti dell'Informatica Spunti di Riflessione in Comparazione con l'Esperienza Statunitense e Francese, in G. Alpa, La Tutela Giuridica del Software, Milano, 1984, p. 80; V.Zeno Zencovich, I Contratti di Informatica. Profili Civilistici Tributari e di Bilancio, Milano,1987, p. 222 e M.A. Monanni, Tutela del Software e Diritto D'Autore. Convergenze e Interferenze, pp. 11-13.

Esistono però dei software che mettono a disposizione degli utenti anche il file sorgente, sono detti "*software open source*".

1.3 Definizione di Intelligenza Artificiale

Ultimamente il termine Intelligenza Artificiale è entrato nel nostro linguaggio quotidiano, ma risulta sempre difficile darne una definizione univoca. In termini generici, possiamo sostenere che si tratta dello studio di come far attuare a processi automatizzati attività tipiche della mente umana.

L'Intelligenza Artificiale può essere definita come un insieme di sistemi software (ed eventualmente hardware) progettati dall'uomo che, dato un obiettivo complesso, agiscono nella dimensione fisica o digitale percependo il proprio ambiente attraverso l'acquisizione di dati, interpretando i dati strutturati o non strutturati raccolti, ragionando sulla conoscenza o elaborando le informazioni derivate da questi dati e decidendo le migliori azioni da intraprendere per raggiungere l'obiettivo dato.

I sistemi di AI possono usare regole simboliche o apprendere un modello numerico e possono anche adattare il loro comportamento analizzando gli effetti che le loro azioni precedenti hanno avuto sull'ambiente.

Come disciplina scientifica, l'AI comprende diversi approcci e diverse tecniche, come l'apprendimento automatico (di cui l'apprendimento profondo e l'apprendimento per rinforzo sono esempi specifici), il ragionamento meccanico (che include la pianificazione, la programmazione, la rappresentazione delle conoscenze e il ragionamento, la ricerca e l'ottimizzazione) e la robotica (che comprende il controllo, la percezione, i sensori e gli attuatori e l'integrazione di tutte le altre tecniche nei sistemi cyberfisici).

Nel seguito del presente lavoro ne verranno illustrate in maniera più dettagliate le principali capacità e criticità.

CAPITOLO 2 – LE VARIE FORME DI PROTEZIONE DI ALGORITMI E SOFTWARE *a cura di Adele Necchia*

http://www.ifarma.net/farmindustria-brevetti/

2.1 Protezione dell'algoritmo

Abbiamo detto che per algoritmo deve intendersi una sequenza finita di istruzioni necessarie per risolvere un problema o raggiungere un determinato obiettivo. L'algoritmo può essere utilizzato in innumerevoli campi. È possibile che un tale algoritmo abbia un uso pratico in molteplici funzioni diverse. Anche una ricetta di cucina può essere definita come algoritmo in quanto è una descrizione generale delle operazioni che devono essere compiute per arrivare ad un determinato risultato (cioè per risolvere un determinato problema). La ricetta (l'algoritmo) rimane la stessa anche variando la quantità degli ingredienti (per 3 persone, per esempio), e può essere usata da un qualsiasi cuoco.

È ormai pacifico che gli algoritmi su cui si basano le AI siano dei veri e propri "metodi matematici" ai sensi della Convenzione sulla Concessione dei Brevetti Europei siglata a Monaco nel 1973 (di seguito anche "CBE"), che ne stabilisce la non brevettabilità (al pari delle scoperte e teorie scientifiche). L'articolo 52 CBE, infatti, tutela le invenzioni "che siano nuove, implichino un'attività inventiva e siano atte ad avere un'applicazione industriale", escludendo esplicitamente i metodi matematici da tale categoria.

Quando si tratta di proprietà intellettuale, è necessario infatti tenere conto di due esigenze contrapposte. Da un lato abbiamo l'importanza di remunerare il creatore dell'invenzione, in modo da incentivarne il lavoro. Dall'altro, le opere dell'ingegno sono beni immateriali e, quindi, non rivali: il loro utilizzo simultaneo da parte di più soggetti non ne diminuisce il valore, anzi, aumenta la possibilità che altri individui, a partire da quell'opera, arrivino a creare nuove invenzioni. Questa caratteristica delle opere dell'ingegno ne rende auspicabile la libera circolazione, che viene però limitata dai diritti di proprietà intellettuale. Alla base dell'esclusione dell'articolo 52 CBE c'è proprio l'esigenza di favorire lo scambio di informazioni, che nei casi di "conoscenza basilare" (si pensi a un teorema scientifico!) prevale sull'importanza di remunerare il creatore.

Tuttavia, il paragrafo 3 dell'articolo 52 CBE contiene le premesse per la brevettabilità di algoritmi che siano utilizzati come parte di un sistema di AI che contribuisce a produrre un effetto tecnico ulteriore: se il metodo matematico è parte di un sistema più complesso, che abbia tutti gli elementi delle invenzioni stabiliti nel primo paragrafo dell'articolo 52 CBE (novità, attività inventiva e applicazione industriale), allora l'intero sistema è brevettabile, comprensivo del metodo matematico utilizzato.

Posto quindi che un algoritmo può avere una tutela giuridica solo in quando comporta un effetto tecnico e si pone come soluzione nuova ad un problema tecnico, esaminiamo quindi le forme di tutela del software.

2.2 La protezione del software: contesto storico

Come anticipato nei paragrafi precedenti, dalla definizione di software[5] si evince che il software appartiene alla categoria dei beni giuridici immateriali in quanto:

a) si tratta di un bene che non è consumabile e dunque non è soggetto a usura;
b) può essere utilizzato simultaneamente da un numero indefinito di persone senza che si verifichi una menomazione della sua utilità.

Per questo motivo, dal punto di vista giuridico, il software può essere classificato come una creazione intellettuale e, come tale, potrà ricevere due tipologie di protezione:

[5] Si intende per software "*l'espressione di un insieme organizzato e strutturato di istruzioni in qualsiasi forma o su qualunque supporto capace, direttamente o indirettamente, di far eseguire o far ottenere una funzione o un compito o far ottenere un risultato particolare per mezzo di un sistema di elaborazione elettronica dell'informazione*" (OMPI, 1984).

a) proteggibilità come invenzione industriale, tutelata attraverso il brevetto;
b) tutela tramite il diritto d'autore o copyright, come opera dell'ingegno di carattere creativo.

Nel panorama europeo, la brevettabilità del software è apparsa sin dall'inizio problematica.

La Convenzione sul Brevetto Europeo (CBE) del 5 ottobre 1973 all'art. 52(1)-(3) recita:

"I brevetti europei sono concessi per le invenzioni in ogni campo tecnologico, a condizione che siano nuove, implichino un'attività inventiva e siano atte ad avere un'applicazione industriale.

Non sono considerate invenzioni ai sensi del paragrafo 1 in particolare:

a) le scoperte, le teorie scientifiche e i metodi matematici;
b) le creazioni estetiche;
c) i piani, principi e metodi per attività intellettuali, per giochi o per attività commerciali, come pure i programmi informatici;
d) le presentazioni di informazioni.

Il paragrafo 2 esclude la brevettabilità degli oggetti o delle attività che vi sono enumerati soltanto nella misura in cui la domanda di brevetto europeo o il brevetto europeo concerna uno solo di tali oggetti o attività, considerati come tali."

Quindi, circa la concessione di brevetti europei, la CBE stabiliva che i programmi per elaboratori "in quanto tali" non possono costituire oggetto di brevetto.

Detto orientamento era dovuto ad una serie di circostanze: la convinzione che la brevettabilità dovesse riguardare la parte hardware di un computer e non all'intangibile ed il timore che i brevetti sul software potessero costituire un ostacolo alla vendita dell'hardware. Infatti, bisogna considerare che inizialmente al software non veniva riconosciuta autonoma importanza, poiché le imprese investivano principalmente sull'hardware e gli elaboratori venivano forniti già completi della componente software (in formato sorgente, in modo da permettere all'utente di adattarlo alle proprie esigenze). La protezione del software veniva assicurata contrattualmente con la vendita del computer oppure mediante mezzi tecnici che impedivano di copiare i programmi[6].

[6] Cnf. https://www.iprights.it/proprieta-intellettuale-software/

Negli anni Settanta, invece, il software comincia ad acquisire maggiore importanza in quanto diventa uno strumento fondamentale nell'aumento della velocità di elaborazione al punto da rappresentare una minaccia all'aumento di velocità consentito dall'hardware (seconda legge di Moore).[7]

In quegli anni, nascono aziende produttrici esclusivamente di software e vengono stanziati cospicui investimenti nell'informatica.

Inoltre, la grande facilità di copiare il software da parte dei contraffattori ed una considerevole rapidità di diffusione del software illecitamente copiato, mediante i floppy disk, allarmava gli operatori del settore[8].

Si rendeva pertanto necessario, anche sul piano giuridico, un maggiore approfondimento per garantire la migliore tutela del software. Infatti, la tutela contrattuale del software era efficace solo fra le parti del contratto. Il software necessitava invece di una protezione che potesse essere fatta valere nei confronti di chiunque, non solo verso gli acquirenti di un personal computer[9].

Inizia, dunque, a partire dagli anni Settanta, il dibattito giuridico sulla natura del software e, quindi, su quale particolare forma di protezione dovesse essere garantita.

In quanto bene immateriale, lo strumento di tutela del software ricade necessariamente nell'ambito della proprietà intellettuale, tuttavia, accanto a chi sosteneva che il software avesse una natura tecnica e che potesse, quindi, essere protetto come un'invenzione, vi era chi lo considerava come un modo di espressione della mente umana paragonabile ad un testo scritto.

Inizialmente, fu questa seconda soluzione a prevalere e ciò principalmente per ragioni di tipo economico: si temeva che la protezione offerta dal brevetto fosse troppo forte e potesse in qualche modo generare dei monopoli ed ostacolare la concorrenza. Conseguentemente, lo sviluppo dell'informatica sarebbe stato molto più lento. La libera concorrenza nel mercato dei software permette una evoluzione più rapida: per restare sul mercato occorre sviluppare software sempre migliori e più performanti.

---

[7] In quegli anni Gordon Moore, che sarà poi cofondatore di Intel, elabora delle osservazioni (c.d. leggi di Moore) derivanti dall'osservazione empirica dei fattori tecnici ed economici i fattori tecnici ed economici che consentono lo sviluppo esponenziale della microelettronica. La prima legge di Moore stabilisce che "il costo delle apparecchiature per fabbricare semiconduttori raddoppia ogni quattro anni". La seconda specifica che "il costo di una fabbrica di chip raddoppia da una generazione all'altra". Con la seconda legge si cominciò a ragionare sull'osservazione della dinamica dei costi legati alla costruzione delle nuove fabbriche di chip, poiché questi costi erano cresciuti ad un ritmo superiore rispetto all'incremento di potenza dei processori.

[8] R. Pietrabissa e M. Barbieri, Brevetti e proprietà industriale, Maggioli Editore, p. 187-194.

[9] Cnf. https://www.filodiritto.com/tutela-del-software-diritto-dautore-brevetto-e-principio-dellesaurimento

La prima legislazione ad inquadrare il software come opera protetta dal diritto d'autore è stata quella statunitense: nel 1980 negli Stati Uniti il "Copyright Act" fu emendato con il "Computer software Amendment" e il software fu incluso come opera protetta.

Similmente, anche alcuni stati europei come la Gran Bretagna e la Francia aderirono a tale orientamento fino ad arrivare alla Direttiva 1991/250/CE (a cui l'Italia ha dato attuazione nel 1992, con il D.lgs. n. 518 del 29/12/1992), che ha introdotto a livello comunitario il software tra i beni tutelabili dal diritto d'autore.

Successivamente, si iniziò a constatare che la protezione tramite diritto d'autore a volte non era adeguata al software in quanto, se da un lato consentiva di tutelare la forma espressiva di un programma, dall'altro non garantiva alcuna protezione dell'idea di base che costituisce il vero valore di un software.

Fu così che negli anni Ottanta si cominciò ad ipotizzare di proteggere il software con il brevetto.

2.3 La tutela tramite diritto d'autore

Nell'ordinamento italiano, i programmi per elaboratore sono tutelati dalla legge sul diritto d'autore (Legge 22 Aprile 1941, n. 633, "*Protezione del diritto d'autore e di altri diritti connessi al suo esercizio*", di seguito "LDA"), così come modificata dal D.lgs. 29 dicembre 1992 n. 518 in attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore. L'articolo 1 di questa legge recita:

"*1. Sono protette ai sensi di questa legge le opere dell'ingegno di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione.*

2. Sono altresì protetti i programmi per elaboratore come opere letterarie ai sensi della Convenzione di Berna sulla protezione delle opere letterarie ed artistiche ratificata e resa esecutiva con legge 20 giugno 1978, n. 399, nonché le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore."

Da tale articolo, risulta che i programmi per elaboratori, vale a dire i software, sono esplicitamente citati dalla legge sul diritto d'autore e sono equiparati da un punto di vista legislativo alle opere letterarie, ossia alle poesie, ai romanzi, etc.

L'articolo 2 continua:

"*In particolare, sono comprese nella protezione:*
1) le opere letterarie, drammatiche, scientifiche, didattiche, religiose, tanto se in forma scritta quanto se orale;

[…]

8) i programmi per elaboratore, in qualsiasi forma espressi purché originali quale risultato di creazione intellettuale dell'autore. Restano esclusi dalla tutela accordata dalla presente legge le idee e i principi che stanno alla base di qualsiasi elemento di un programma, compresi quelli alla base delle sue interfacce. Il termine programma comprende anche il materiale preparatorio per la progettazione del programma stesso. …"

Dal combinato disposto dei suddetti articoli si evince che un requisito fondamentale per la protezione del diritto d'autore è quello che il programma per elaboratore sia "*opera dell'ingegno di carattere creativo*", ovvero sia originale rispetto alle opere preesistenti. Il programma deve quindi essere stato pensato e sviluppato autonomamente dall'autore.
Con il concetto di "creatività" si intende la creatività semplice, riscontrabile in tutti i casi in cui l'autore abbia operato una scelta discrezionale all'interno di un ambito di diverse alternative, attraverso le quali esprimere i contenuti.
Vanno quindi escluse dalla tutela solo le forme espressive caratterizzate dalla mera funzionalità, banali o standardizzate, che non consentono di apprezzare nemmeno un minimo livello di creatività e originalità.
Tuttavia, spesso è difficile stabilire se, rispetto ad altri prodotti già sviluppati, il software consista in un'elaborazione talmente creativa da costituire un'opera autonoma oppure, sia una mera riproduzione di un programma altrui con l'aggiunta di alcune varianti di natura secondaria.
Al riguardo, la Corte di Cassazione ha più volte affermato che la creatività e l'originalità sussistono anche qualora l'opera sia composta da idee e nozioni semplici, comprese nel patrimonio intellettuale di

persone aventi esperienza nella materia propria dell'opera stessa, purché formulate ed organizzate in modo personale ed autonomo rispetto alle precedenti[10].

L'articolo 2 della LDA enuncia anche i limiti della tutela conferita dal diritto d'autore: con il diritto d'autore viene tutelato il codice sorgente, il codice oggetto (ossia la traduzione del linguaggio del programma in bit o linguaggio macchina) e il materiale preparatorio (es. i diagrammi di flusso), ma non le idee ed i principi in sé alla base del codice sorgente od oggetto di un programma.

Quindi, la tutela del programma per elaboratore mediante il diritto d'autore, da un lato, protegge l'espressione dei programmi in una qualsiasi forma concreta, dall'altro esclude dalla tutela le idee in quanto tali, e quindi le soluzioni e i principi che caratterizzano il software, compresi quelli inerenti alla sua interfaccia.

Non è possibile vantare un'esclusiva su concetti generali alla base del programma per elaboratore.

Per esempio, l'autore di un romanzo con una trama relativa ad un intrigo internazionale con sfondo psicologico non può pretendere una esclusiva su una tematica così generica[11].

Ugualmente per i software, chiunque potrà realizzare un software avente una funzione analoga a quello creato, purché lo faccia senza copiare il codice sorgente ed il codice oggetto.

Con tale orientamento si è, pertanto, ritenuto di proteggere i singoli programmi senza arrestare il processo di innovazione tecnologica e scientifica, ossia consentendo la libera diffusione di idee, principi e algoritmi che stanno alla base del software.

Analogamente a quanto avviene per le opera letterarie, il diritto d'autore sul software si divide in una componente morale, che rimane sempre attribuita all'autore del programma, e in una di natura patrimoniale che consiste essenzialmente nei diritti di utilizzazione economica (cioè il diritto di pubblicare, diffondere e commercializzare il software) e può essere oggetto di cessione.

[10] Corte di Cassazione, sentenza n. 581 del 12 gennaio 2007: in particolare la Cassazione, affermando che per la protezione del diritto d'autore sul software, al pari di quello riguardante qualsiasi altra opera, è necessario il requisito dell'originalità, si pone la necessità di stabilire se l'opera (ossia il programma) sia o meno frutto di un'elaborazione creativa originale rispetto ad opere precedenti. Pertanto, la Cassazione stabilisce al riguardo: che la creatività e l'originalità sussistono anche qualora l'opera sia composta da idee e nozioni semplici, comprese nel patrimonio intellettuale di persone aventi esperienza nella materia propria dell'opera stessa, purché formulate ed organizzate in modo personale ed autonomo rispetto alle precedenti; e che la consistenza in concreto di tale autonomo apporto forma oggetto di una valutazione destinata a risolversi in un giudizio di fatto, come tale sindacabile in sede di legittimità soltanto per eventuali vizi di motivazione (si vedano tra le altre, anche Cassazione 20925/05, e 11953/93). Ne consegue, pertanto, che la specificità di un programma software che pure presenti un'architettura di base comune ad altri sistemi risiede nella capacità di adattare l'architettura applicativa al caso ed all'ambiente tecnologico specifico.

[11] R. Pietrabissa e M. Barbieri, Brevetti e proprietà industriale, Maggioli Editore, p. 187-194.

Come previsto dall'articolo 6 della LDA, entrambe le componenti nascono per il fatto stesso della creazione del programma, automaticamente al momento dell'incorporazione dell'opera sul supporto materiale che ne permette l'individuazione, senza alcuna formalità (deposito o registrazione).

I diritti morali sono inalienabili, non espropriabili, non sottoponibili a condizioni o rinunce e comprendono:

a) diritto alla paternità dell'opera;
b) diritto di inedito;
c) diritto alla integrità dell'opera;
d) diritto di ritiro dell'opera per gravi ragioni morali.

Il diritto alla paternità dell'opera consiste nel diritto di essere pubblicamente indicato e riconosciuto come creatore dell'opera, di cui può rivendicare in qualunque momento la paternità (art. 20 LDA).

Nell'ambito di questo diritto rientra anche la facoltà dell'autore di far circolare la propria opera in forma anonima o con uno pseudonimo, conservando il diritto di rivelarsi e di far riconoscere in giudizio, in qualsiasi momento, la sua qualità di autore (art. 21 LDA).

L'autore può esercitare tale diritto sia rivendicando a sé la paternità della sua opera, sia con il pretendere che il proprio nome sia apposto sugli esemplari della sua opera in circolazione.

Ne deriva che l'autore di un'opera può essere esclusivamente una persona fisica stante la concreta impossibilità di ricondurre in capo ad una persona giuridica l'espressione di un'attività creativa[12]. Peraltro, qualsiasi contratto o dichiarazione unilaterale in cui l'autore rinunzi ai suoi diritti morali deve considerarsi nullo ed improduttivo di effetti giuridici poiché, come anticipato, il diritto morale d'autore costituisce un diritto indisponibile e quindi irrinunziabile[13].

Il diritto di inedito consiste nella facoltà dell'autore di decidere se e quando pubblicare la sua opera, potendo anche lasciarla per sempre inedita od opporsi alla prima pubblicazione, recedendo da contratti che l'abbiano autorizzata. Il diritto di inedito si esaurisce con la pubblicazione dell'opera. Se l'autore ha espressamente vietato la pubblicazione di una sua opera, neppure gli eredi, alla sua morte, possono esercitare questo diritto (art. 24 LDA), che può essere espropriato solo per ragioni di interesse dello Stato (art. 112 LDA).

[12] Cnf. https://www.diritto.it/la-tutela-del-software-opera-dellingegno/
[13] Cnf. https://www.diritto.it/la-tutela-del-software-opera-dellingegno/

Il diritto all'integrità dell'opera invece rappresenta il diritto dell'autore di opporsi a qualsiasi deformazione, mutilazione o altra modificazione, nonché a qualsiasi atto che possa recare pregiudizio al suo onore o alla sua reputazione: chi crea un'opera ha il diritto di essere giudicato dal pubblico per l'opera così come l'ha concepita e di conservare la reputazione che deriva dalla corretta conoscenza della stessa.

Questo diritto tutela non solo le modifiche dell'opera ma anche qualsiasi modalità di comunicazione che ne possa cambiare la percezione e quindi il giudizio da parte del pubblico, come ad esempio l'utilizzazione dell'opera per la promozione o per la pubblicità di determinati prodotti. L'autore non può impedire l'esecuzione delle modifiche alla sua opera o chiederne la soppressione quando ne abbia avuto conoscenza e le abbia accettate (art. 22, comma 2 LDA).

Dopo la morte dell'autore, il diritto morale può essere fatto valere, senza limite di tempo, dal coniuge e dai figli e, in loro mancanza, dai genitori e dagli altri ascendenti e dai discendenti diretti; mancando gli ascendenti ed i discendenti, dai fratelli e dalle sorelle e dai loro discendenti (art. 23 LDA).

La violazione del diritto morale costituisce illecito tutelabile quando la violazione del diritto morale è commessa insieme alla violazione di uno dei diritti di sfruttamento economico.

I diritti patrimoniali sono i diritti esclusivi dell'autore di utilizzare economicamente la sua opera in ogni forma e modo, originale o derivato (art. 12 LDA; art. 2577 c.c.) e di percepire un compenso per ogni tipo di utilizzazione della stessa.

A differenza dei diritti morali, i diritti patrimoniali sono rinunciabili, possono essere oggetto di cessione a terzi (art. 107 LDA; art. 2581 c.c.). Solitamente, la cessione è a titolo oneroso, ma è possibile anche gratuitamente.

I diritti patrimoniali sono tra loro indipendenti (art. 19 LDA): l'esercizio di uno di essi non esclude l'esercizio esclusivo di ciascuno degli altri diritti. Sono, quindi, esercitabili separatamente o congiuntamente e possono avere ad oggetto l'opera nella sua interezza o in ciascuna delle sue parti. Chi acquista un diritto o una facoltà sul programma è quindi legittimato ad usarlo solo in relazione al diritto acquistato.

Inoltre, i diritti patrimoniali durano tutta la vita dell'autore e sino al termine del settantesimo anno solare dopo la sua morte (art. 25 LDA).

L'articolo 64-bis della LDA, introdotto con il D.lgs. n. 518 del 1992, ha specificamente individuato i diritti esclusivi concernenti i programmi per elaboratore. In particolare, viene riservata all'autore del software

la riproduzione del programma, permanente o temporanea, totale o parziale, con qualsiasi mezzo e in qualsiasi forma.

Se le operazioni di caricamento, visualizzazione, esecuzione o memorizzazione richiedono la riproduzione del programma, anche tali operazioni sono soggette all'autorizzazione del titolare del diritto d'autore.

Inoltre, viene riservata all'autore del software la traduzione, l'adattamento, la trasformazione e ogni altra modificazione del programma, nonché la riproduzione dell'opera che ne risulti. Si osserva quindi come il diritto d'autore non solo protegga da una copia identica del software, ma impedisca anche che ne vengano fatti trasformazioni ed adattamenti e tutela anche da copie parziali.

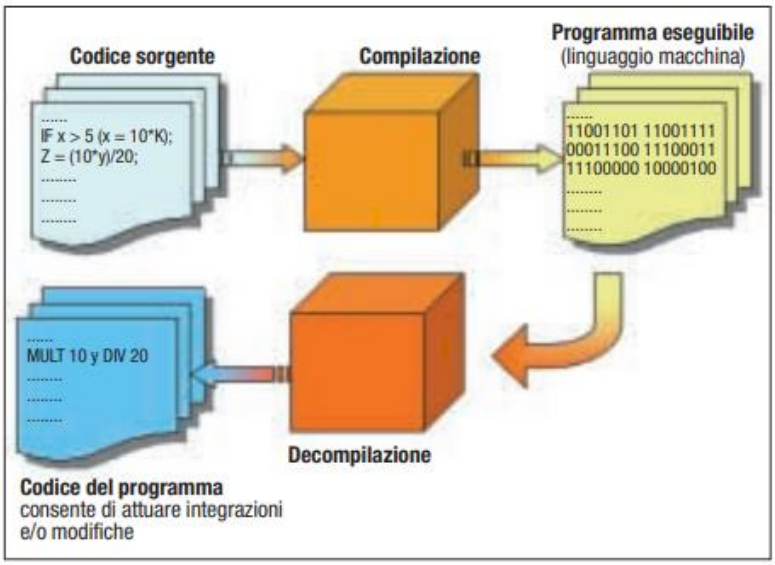
Infine, spetta all'autore qualsiasi forma di distribuzione al pubblico, compresa la locazione e la commercializzazione. In questo ambito, trova applicazione il c.d. principio di esaurimento: con la prima vendita di un programma in ambito comunitario viene esaurito il diritto di distribuzione, cioè non può essere impedita a terzi la successiva vendita di tale programma in tutta l'Unione Europea, sempre nel rispetto dei diritti dell'autore a cui vanno corrisposte le relative royalty.

Le eccezioni a tale esclusiva sono indicate dagli articoli 64-ter e 64-quater.

Nello specifico, l'articolo 64-ter LDA stabilisce che chi ha la possibilità di utilizzare una copia del programma per elaboratore può effettuare una copia di riserva (c.d. copia di backup) ed osservare, studiare o sottoporre a prova il funzionamento del programma. L'attività di analisi deve essere preordinata alla determinazione delle idee e dei principi su cui è basato ogni elemento del programma stesso, qualora egli compia tali atti durante operazioni di caricamento, visualizzazione, esecuzione, trasmissione o memorizzazione del programma che egli ha il diritto di eseguire.

L'art. 64-quater LDA disciplina il tema molto discusso della decompilazione (o reverse engineering), procedimento che, consentendo di risalire dal programma oggetto al programma sorgente, è necessario al fine di sviluppare programmi che possano interagire tra loro e permettere prestazioni più complesse e complete[14].

[14] Cnf. Antonio Piva e David D'Agostino, La tutela giuridica dei programmi per elaboratore.



La problematica della decompilazione si inquadra nell'esigenza di garantire una certa divulgazione delle informazioni tecniche contenute nei programmi per elaboratore, degli algoritmi che ne sono la base, della loro struttura, e in generale di tutte le conoscenze tecniche impiegate nello sviluppo dei programmi, in modo che chi ne venga a conoscenza sia messo in grado di impiegarle per programmi diversi (non sostanzialmente simili), al fine di favorire lo sviluppo tecnologico del settore[15].

È evidente che la conoscenza così ottenuta di nozioni tecniche è un presupposto essenziale per il progresso del settore e per un responsabile uso del programma.

Tale norma è infatti volta ad evitare che si formino posizioni di monopolio nel momento in cui il titolare dei diritti sul software di sistema si possa opporre all'interoperabilità di altri software applicativi, che non siano stati realizzati da lui stesso.

L'articolo dispone che: "*l'autorizzazione del titolare dei diritti non è richiesta qualora la riproduzione del codice del programma di elaboratore e la traduzione della sua forma ... compiute al fine di modificare la forma del codice, siano indispensabili per ottenere le informazioni necessarie per conseguire l'interoperabilità, con altri programmi, di un programma per elaboratore creato autonomamente*", purché siano soddisfatte alcune condizioni previste dalla stessa legge.

In particolare, la decompilazione può essere effettuata:

a) solo se eseguita da chi ha il diritto di usare il software (art. 64 quater comma 1, lett. A LDA);

[15] Cnf. Antonio Piva e David D'Agostino, La tutela giuridica dei programmi per elaboratore.

b) se le informazioni necessarie per conseguire l'interoperabilità non siano già "facilmente reperibili e rapidamente accessibili" (art. 64-quater comma 1, lett. B LDA); se sia limitata solo alle "parti del programma originale necessarie per conseguire l'interoperabilità" (art. 64-quater comma 1, lett. C LDA);
c) se le informazioni acquisite non siano comunicate a terzi (art. 64 quater-comma 2, lett. b LDA);
d) se le informazioni acquisite non siano utilizzate per costruire programmi sostanzialmente simili nella loro forma espressiva (art. 64 quater comma 2, lett. C LDA). L'esercizio di queste attività, difatti, costituirebbe una forma di disposizione dei diritti patrimoniali non autorizzata né da parte del titolare né da parte del legislatore.

Inoltre, il legislatore, con il D.lgs. n. 205 del 15 marzo del 1996, intervenuto a modificare le statuizioni del D.lgs. 518 del 1992, ha stabilito che le clausole contrattuali pattuite in violazione di quanto sopra detto debbono considerarsi nulle.

Come norma di chiusura, viene stabilito che le disposizioni relative alla decompilazione non possono essere interpretate in modo da consentire che la loro applicazione rechi indebitamente pregiudizio agli interessi del titolare del diritto o entri in conflitto con il normale impiego del programma.

Per quanto concerne i soggetti del diritto, in relazione al programma creato da un lavoratore subordinato nell'ambito del suo rapporto lavorativo, i diritti di sfruttamento economico spettano al datore di lavoro. Infatti, l'articolo 12-bis della LDA dispone che:

"*salvo patto contrario, il datore di lavoro è titolare del diritto esclusivo di utilizzazione economica del programma per elaboratore o della banca di dati creati dal lavoratore dipendente nell'esecuzione delle sue mansioni o su istruzioni impartite dallo stesso datore di lavoro*".

Anche il software realizzato per conto di una Pubblica Amministrazione diventa di proprietà di quest'ultima (art. 11 LDA).

Nel caso, invece, in cui il software sia stato realizzato su commissione, la legge non disciplina espressamente chi sia il titolare dei diritti economici sul programma che verrà realizzato per cui è buona regola disciplinare questo aspetto contrattualmente.

Riguardo alle opere collettive[16], titolare del diritto d'autore è chi organizza l'opera, grazie ad una attività di scelta, coordinamento e direzione. L'opera collettiva è quindi la riunione di opere di autori distinti che vengono messe insieme da un altro soggetto che coordina il lavoro nel suo complesso e diviene a sua volta autore, cioè titolare di diritti autonomi e diversi rispetto ai diritti vantati dagli altri sulle singole opere.

Per le opere in comunione[17], ovvero nate tramite il contributo indistinguibile, inscindibile e paritario di più persone, il diritto d'autore sorge in comunione in capo a tutti i creatori dell'opera.

Come precedentemente specificato, il diritto di autore nasce con la creazione stessa del programma e non richiede alcuna ulteriore operazione. Tuttavia, è importante per l'autore poter dimostrare una data esatta di creazione del software da opporre ad eventuali contestazioni di terzi.

Una modalità efficace per fornire all'autore prova della paternità e della data di creazione di un determinato programma è il deposito presso la SIAE (Società Italiana degli Autori ed Editori).

In questo caso, il deposito ha la sola funzione di fissare una data certa, quella del deposito del programma, a partire dalla quale possono essere fatti valere i diritti d'autore sull'opera realizzata. La registrazione è facoltativa, serve esclusivamente a facilitare la prova della titolarità del diritto, in quanto si presume che il soggetto che ha registrato il programma ne sia l'autore. Tale presunzione non è però assoluta, ed è dunque possibile fornire anche la prova contraria.

l tipo di deposito varia a seconda che il programma sia pubblicato oppure no. Nel primo caso, si procede con la registrazione presso il registro pubblico del software tenuto dalla SIAE, mentre nel secondo caso si procede con un normale deposito di opera inedita.

Con il termine "pubblicazione" si intende il primo atto di esercizio dei diritti connessi al software che può essere la prima riproduzione del programma per la commercializzazione o in caso di programma realizzato su commissione il momento della consegna del programma al committente o al datore di lavoro.

Per procedere alla registrazione, occorre predisporre un'apposita domanda nella quale devono essere rappresentati una descrizione del programma che comprenda ogni utile elemento per la sua

[16] Cnf. art. 3 LDA: "*Le opere collettive, costituite dalla riunione di opere o di parti di opere, che hanno carattere di creazione autonoma, come risultato della scelta e del coordinamento ad un determinato fine letterario, scientifico, didattico, religioso, politico od artistico, quali le enciclopedie, i dizionari, le antologie, le riviste e i giornali, sono protette come opere originali indipendentemente e senza pregiudizio dei diritti di autore sulle opere o sulle parti di opere di cui sono composte*".

[17] L'opera in comunione è quell'opera risultante da apporti creativi di più persone che vanno a formare un tutto e in cui non è possibile distinguere il contributo di ciascuno.

identificazione ed alcuni dati relativi all'autore. È necessario, inoltre, il deposito di un esemplare del programma (un CD-ROM che non è consultabile da terzi) ed il pagamento di una tassa di registrazione. Il deposito, una volta effettuato, non deve essere rinnovato. Nel caso in cui il programma abbia delle implementazioni future, anche le nuove versioni del programma dovranno essere registrate.

La SIAE attribuisce ai programmi depositati un numero progressivo e la data di registrazione e fornisce al richiedente un attestato di registrazione. La registrazione sul pubblico registro del software fa fede fino a prova contraria dell'esistenza del programma e di chi ne sia l'autore.

I dati inseriti nell'archivio sono pubblici e possono essere consultati da chiunque ne faccia richiesta. La SIAE rilascia copie autentiche ed estratti di tutto ciò che è depositato tranne dell'esemplare del programma, il quale non è oggetto di visura.

Nel registro possono anche essere trascritti gli atti di trasferimento totale o parziale dei diritti di utilizzazione economica ovvero gli atti che costituiscono su di essi diritti di usufrutto o di garanzia ovvero gli atti di divisione o di società.

Per la loro trascrizione è necessario presentare l'originale o la copia autentica della scrittura privata con firme autenticate da un notaio.

A differenza della registrazione, che, come sopra illustrato, si realizza quando il software sia già stato pubblicato, il deposito di un'opera inedita ricorre invece quando la pubblicazione non sia ancora avvenuta.

Per effettuare il deposito, è necessario compilare un'apposita domanda ed allegare il programma copiato su un supporto magnetico. Mentre in caso di registrazione, il registro è consultabile da chiunque e la SIAE è obbligata a rilasciare estratti o copie autentiche degli atti detenuti, con il deposito di inedito, invece, la SIAE garantisce la riservatezza dell'operazione e si obbliga a non fornire a terzi notizie circa l'esistenza del deposito, la data di effettuazione, il numero di repertorio assegnato. Il deposito permette di avere una prova certa sulla data di creazione.

All'autore o al depositante verrà rilasciato un attestato recante il numero di repertorio assegnato al deposito. Il deposito ha una durata di 5 anni rinnovabile alla scadenza per un uguale periodo, salva la facoltà del titolare di ritirare in ogni momento l'opera.

Se alla scadenza il titolare non ritira l'opera o non rinnova il deposito, la SIAE procede alla distruzione del materiale stesso.

2.4 Tutela tramite brevetto

Riprendendo quanto esaminato nel precedente capitolo sul contesto storico, con la nascita negli anni Settanta di aziende produttrici di solo software e con i sempre più ingenti investimenti delle aziende per lo sviluppo di nuovi programmi in svariati campi tecnologici, si è reso necessario tutelare non solo la forma espressiva del software, ma anche le logiche sottese alla creazione del software stesso.

In particolare, il rischio maggiore è rappresentato dal reverse engineering attraverso il quale sviluppatori possono risalire da un programma al suo diagramma di flusso per poi crearne uno del tutto nuovo che però svolge esattamente le stesse funzioni, con ciò danneggiando il primo sviluppatore[18].

La tutela del software tramite il deposito di una domanda di brevetto consente di proteggere la logica del software, a prescindere dallo specifico linguaggio di programmazione che è stato utilizzato.

L'articolo 52 della Convenzione sulla Concessione dei Brevetti Europei (CBE) stabilisce che:

"(1) European patents shall be granted for any inventions, in all fields of technology, provided that they are new, involve an inventive step and are susceptible of industrial application.

(2) The following in particular shall not be regarded as inventions within the meaning of paragraph 1:

a) *discoveries, scientific theories and mathematical methods;*
b) *aesthetic creations;*
c) *schemes, rules and methods for performing mental acts, playing games or doing business, and programs for computers;*
d) *presentations of information.*

(3) Paragraph2 shall exclude the patentability of the subject-matter or activities referred to therein only to the extent to which a European patent application or European patent relates to such subject-matter or activities as such."

Il primo comma di questo articolo precisa quindi che sono potenzialmente brevettabili le invenzioni in tutti campi della tecnologia.

Nel successivo comma 2, si elencano le materie che non sono considerate invenzioni, fra le quali sono annoverati anche i programmi per elaboratore.

[18] Cnf. https://www.ufficiobrevetti.it/software/

Il comma 2 infine afferma che il divieto alla brevettazione riguarda i brevetti e le domande di brevetto che si riferiscono alle materie di cui al comma 2 considerate in quanto tali ("*as such*")[19] ma non in modo assoluto.

Tale impostazione è ripresa anche dall'articolo 45 della LDA che recita:

"*(1) Possono costituire oggetto di brevetto per invenzione le invenzioni, di ogni settore della tecnica, che sono nuove e che implicano un'attività inventiva e sono atte ad avere un'applicazione industriale.*

(2) Non sono considerate come invenzioni ai sensi del comma 1 in particolare:

a) le scoperte, le teorie scientifiche e i metodi matematici;

b) piani, i principi ed i metodi per attività intellettuali, per gioco o per attività commerciale ed i programmi di elaboratore;

c) le presentazioni di informazioni.

(3) Le disposizioni del comma 2 escludono la brevettabilità di ciò che in esse è nominato solo nella misura in cui la domanda di brevetto o il brevetto concerne scoperte, teorie, piani, principi, metodi, programmi e presentazioni di informazioni considerati in quanto tali".

Quindi, sia la Convenzione sul Brevetto Europeo (art. 52) che il Codice della Proprietà Industriale italiano (art. 45) escludono la brevettabilità del software solo se considerato "in quanto tale" ("as such"), ma non in modo assoluto. Si pone quindi il problema, sia in ambito europeo che in ambito italiano, di comprendere quando una creazione correlata ad un software possa o meno essere considerata "un software in quanto tale".

Per risolvere la questione è necessario soffermarsi sull'espressione "*shall be granted for any inventions, in all fields of technology*", che evidenzia come l'invenzione debba possedere intrinsecamente un carattere tecnico.

[19] Emanuela Arezzo, La brevettabilità del software e dei metodi commerciali elettronici nella giurisprudenza dell'Ufficio Europeo Brevetti: "*La ragione esatta per cui il software fu inserito nella lista delle c.d. non invenzioni non è ad oggi chiara. L'unico sistema legislativo che vietava espressamente la brevettabilità del software era quello francese (art. 7, loi 68 – l del 2 gennaio 1968). Nessun altro Paese europeo contemplava un tale veto nell'ambito della propria legislazione prima del suo inserimento all'interno della CBE40. All'epoca, i programmi per elaboratore venivano spesso considerati alla stregua di conoscenze matematiche (l'insieme di istruzioni che forma un programma si fonda, infatti, su algoritmi matematici) e quindi di saperi astratti. Probabilmente, il legislatore dell'epoca temeva che la tutela brevettuale avrebbe garantito un monopolio estremamente forte che, se caduto in mano di poche grandi imprese, avrebbe ostacolato lo sviluppo di un settore industriale ancora agli albori41. La decisione dell'inserimento dei programmi per elaboratore nella lettera c) dell'art. 52 (2) CBE fu quindi, probabilmente, una scelta strategica motivata dal principale intento di favorire il sorgere di un'industria informatica europea*".

Pertanto, secondo la linea interpretativa dell'Ufficio europeo dei brevetti (EPO), i programmi per elaboratore "in quanto tali" rappresenterebbero concetti puramente astratti, privi di implicazione tecnica (decisione dell'EPO T 258/03). Ad esempio, non possono essere brevettati i software gestionali o di calcolo.

L'esclusione dalla brevettabilità non si applicherebbe ai programmi per elaboratore dotati di un carattere tecnico, cioè a quei programmi per elaboratore in grado di produrre un effetto tecnico ulteriore che va al di là della normale interazione tra il software e l'hardware sul quale viene tale software è eseguito (decisione dell'EPO T 1173/97).

Da ciò deriva che l'espressione "programma per elaboratore in quanto tale" deve interpretarsi come "programma per elaboratore privo di carattere tecnico".

Quindi, anche se gli articoli della CBE relativi ai requisiti di brevettabilità menzionano solo novità, attività inventiva e applicabilità industriale e non introducono un requisito relativo al contenuto tecnico, il carattere tecnico emerge come un prerequisito che consente di stabilire se, in primo luogo, un trovato possa considerarsi o meno come rientrante nella categoria generale delle invenzioni.

Il software può, quindi, rappresentare un elemento tecnico concreto, sotto forma di processore programmato, che interagisce con altri componenti di una macchina per controllarne certe funzionalità, diventando pertanto un mezzo tecnico che risolve un problema tecnico e come tale potendo essere brevettato[20].

Sin dalla fine degli anni Ottanta la giurisprudenza dell'UEB ha iniziato a dar spazio alla tutela brevettuale là dove quei trovati, apparentemente non brevettabili ai sensi dell'art. 52(2) CBE, si dimostrassero in possesso di carattere tecnico divenendo, quindi, "invenzioni" ai sensi dell'art. 52 (1).

La prima decisione che ha ammesso la brevettabilità di un'invenzione attuata attraverso l'elaboratore elettronico è stata Vicom/Computer – Related Invention. La società VICOM System Inc. depositò in data 22.05.1979 una domanda di brevetto relativa a un programma per computer in grado di processare dati contenenti informazioni relative ad immagini, di modificare tali dati e, quindi, di mostrare il risultato dell'immagine così alterata sul monitor; il tutto attraverso l'impiego di un particolare algoritmo. L'invenzione venne rivendicata come metodo per l'elaborazione digitale delle immagini, nonché come apparato programmato per dare attuazione al procedimento rivendicato. La Divisione

[20] Cnf. https://www.ufficiobrevetti.it/software/

d'Esame dell'UEB respinse la domanda di brevetto in quanto ritenne che la rivendicazione di metodo avesse ad oggetto un mero metodo matematico e, dunque, andasse considerata come diretta a richiedere protezione per un programma per computer in quanto tale. La società promosse appello. La Camera dei Ricorsi dell'UEB esaminò le rivendicazioni e trovò che l'invenzione non si riferisse a un mero metodo matematico, bensì a un procedimento tecnico capace di produrre un risultato di natura tecnica. Questa decisione rivoluzionò l'approccio dell'UEB in merito a questo tipo di invenzioni, sancendo il principio della tecnicità.

Anche se il significato "tecnico" o "non tecnico" è meno ambiguo di quello derivante dall'espressione "in quanto tale", tuttavia si deve osservare che non esiste una definizione univoca di "tecnico" che permetta di individuare con oggettività e uniformità se vi sia o meno tecnicità in un determinato programma per elaboratore[21].

Nel corso degli anni, le sentenze della Camere dei ricorsi dell'UEB hanno chiarito che il software può essere suscettibile di brevetto allorché il suo effetto tecnico superi la normale interazione fisica tra il programma in sé ed il computer stesso[22], derivante da puri stimoli elettronici, e che invece porti ad alterare il funzionamento tangibile della macchina/apparato in un campo che non sia escluso dal brevettabile né sia avulso dai settori della tecnica. In sintesi, il software sarà brevettabile se ha un carattere tecnico, ossia se apporta una soluzione tecnica ad un problema tecnico e se ottiene un effetto tecnico. Ovviamente, oltre al carattere tecnico, per la brevettabilità del software dovranno anche essere rispettati gli altri requisiti di brevettabilità.

L'Ufficio Brevetti Europeo ed i giudici europei hanno infatti concesso alcuni brevetti per le cc. dd. "software implemented inventions". Nella giurisprudenza europea, queste possono dividersi in a) invenzioni nelle quali il programma produce un effetto tecnico interno al computer o ad altri sistemi di elaborazione e b) invenzioni in cui un programma gestisce, tramite il computer, un apparato o un procedimento industriale esterno al computer, risultando dunque nell'applicazione dell'informatica alla soluzione di problemi tecnici.

Quando l'invenzione, per cui si richiede il brevetto, presenta i requisiti richiesti dalla legge, allora sarà attribuito al titolare dell'invenzione il diritto al riconoscimento morale dell'invenzione ed il diritto allo

[21] R. Pietrabissa e M. Barbieri, Brevetti e proprietà industriale, Maggioli Editore, p. 187-194.
[22] Cnf. T 1173/97, T 931/95 e T 641/00.

sfruttamento patrimoniale dell'invenzione stessa in via esclusiva. Come detto, il diritto morale è inalienabile, mentre i diritti patrimoniali sono alienabili e trasmissibili.

Resta inteso, che qualora il software non soddisfi tale requisito, e non sia quindi brevettabile, può essere in ogni caso protetto mediante il diritto d'autore.

Circa l'elemento soggettivo, anche per il brevetto dobbiamo analizzare la disciplina prevista per le invenzioni dei lavoratori dipendenti. Nella fattispecie, distinguiamo tre tipologie:

a) le invenzioni di servizio;
b) le invenzioni di azienda;
c) le invenzioni occasionali.

Nel primo caso, si profila l'ipotesi in cui l'invenzione è posta in essere dal lavoratore dipendente che svolge attività di lavoro di ricerca volta all'invenzione. Lo svolgimento della predetta attività lavorativa è parte sostanziale delle attività oggetto del contratto di lavoro. L'attività lavorativa in questione deve essere oggetto di specifica retribuzione. Se questi criteri sono rispettati, la titolarità dell'invenzione di servizio, con gli annessi diritti patrimoniali, sarà di titolarità del datore di lavoro, salvo il diritto dell'inventore di essere riconosciuto autore.

Per quanto concerne le invenzioni di azienda, la disciplina è lievemente differente: l'attività inventiva non è oggetto del contratto che lega il dipendente al datore di lavoro e l'invenzione viene realizzata in esecuzione dell'adempimento di un contratto di lavoro. La titolarità dell'invenzione, con i relativi diritti patrimoniali, spetterà al datore di lavoro, salvo il diritto del lavoratore di esserne riconosciuto autore e ricevere un equo premio.

Nella fattispecie, nel momento in cui una invenzione viene qualificata come invenzione di azienda comporta il diritto per il dipendente, inventore del trovato, di ricevere da parte del datore di lavoro un equo premio, "*tenendo conto dell'importanza dell'invenzione, delle mansioni del svolte e della retribuzione percepita dall'inventore, nonché del contributo che questi ha ricevuto dall'organizzazione del datore di lavoro*".

Sul punto, la maggior parte della giurisprudenza ritiene che l'elemento distintivo fra le due ipotesi (invenzione di servizio e le invenzioni di azienda) risieda precipuamente nella presenza o meno di una

esplicita previsione contrattuale di una speciale retribuzione costituente corrispettivo dell'attività inventiva[23].

Le invenzioni occasionali sono invece realizzate dal dipendente al di fuori del rapporto di lavoro, pur rientrando nel campo di attività del datore di lavoro. Il diritto morale e patrimoniale scaturente dall'invenzione spetta all'inventore, anche se il datore di lavoro ha il diritto di opzione per l'uso esclusivo e non esclusivo dell'invenzione o per l'acquisto del brevetto.

2.5 Le due forme di tutela a confronto

Come detto, il software può essere tutelato sia con il diritto d'autore che con il brevetto. Queste due forme di tutela non sono fra di loro in contrasto, ma sono cumulabili in quanto rivolte a proteggere caratteristiche diverse dello stesso prodotto.

Per quanto riguarda il diritto d'autore, questo tutela sostanzialmente la forma espressiva del software (intesa come sequenza di istruzioni), e non i contenuti e le idee su cui si basa. Dunque, ad essere protetti da copyright sono il codice sorgente ed il codice oggetto, ma non la loro funzione. Questa forma di protezione fornisce una tutela molto efficace nei confronti delle copiature o di riproduzioni illecite di copie, ma non protegge contro la riscrittura del programma: quindi chiunque potrà realizzare un software avente una funzione analoga a quello già creato, purché lo faccia senza copiare il codice sorgente ed il codice oggetto[24].

Per quanto riguarda lo strumento brevettuale, il brevetto per invenzione tutela la logica del software, indipendentemente dalla sua forma espressiva.

Il brevetto consente di proteggere ciò che è rivendicato nella domanda di brevetto e quindi conferisce una tutela più ampia rispetto a quella ottenibile dal diritto d'autore, in quanto con le rivendicazioni è possibile tutelare anche i principi e le idee poste alla base del software.

I brevetti conferiscono al suo titolare un diritto esclusivo sull'invenzione, in un tempo ed in un luogo determinati, impedendo di produrli o diffonderli senza autorizzazione. È pur vero che la durata del

[23] Da: https://link.springer.com/chapter/10.1007/978-3-662-62179-0_2

[24] Da: https://www.iprights.it/proprieta-intellettuale-software/

brevetto è inferiore a quella del diritto d'autore ed è necessario effettuare un deposito presso un ufficio competente.

In conclusione, è possibile tutelare giuridicamente il software scegliendo o cumulando queste due tipologie di tutela, che, come illustrato nei precedenti paragrafi, sono diverse nei modi di acquisizione del diritto[25], nella durata del diritto e per gli strumenti di difesa a disposizione in caso di violazione dello stesso.

2.6 Tutela tramite segreto dell'algoritmo e del software

Al giorno d'oggi, molte aziende scelgono di classificare un algoritmo o un software come segreto commerciale come prima linea di difesa.

A livello normativo, l'ordinamento italiano dedica due norme alla specifica tutela di queste informazioni: gli articoli 98 e 99 del Codice della proprietà industriale (di seguito "CPI"). Inoltre, anche le regole che sanzionano la concorrenza sleale ex art. 2598 c.c. possono essere utilizzate per ottenere una protezione.

L'art. 98 del Codice della proprietà industriale stabilisce che:

"*Per segreti commerciali si intendono le informazioni aziendali e le esperienze tecnico-industriali, comprese quelle commerciali, soggette al legittimo controllo del detentore, ove tali informazioni:*

a) siano segrete, nel senso che non siano nel loro insieme o nella precisa configurazione e combinazione dei loro elementi generalmente note o facilmente accessibili agli esperti ed agli operatori del settore;

b) abbiano valore economico in quanto segrete;

c) siano sottoposte, da parte delle persone al cui legittimo controllo sono soggette, a misure da ritenersi ragionevolmente adeguate a mantenerle segrete."

Per know-how aziendale deve intendersi l'insieme delle informazioni e conoscenze tecnico-industriali e commerciali di una data impresa, sviluppate internamente e/o altrimenti acquisite, e che sono sintesi di tutto ciò che sta a monte di un dato prodotto o di un metodo produttivo.

[25] I diritti sull'invenzione industriale sorgono nel momento del conseguimento del brevetto, mentre i diritti d'autore sulle opere di ingegno sorgono nel momento stesso della creazione dell'opera.

Pertanto, qualora rivestano un carattere strategico per il business dell'azienda o qualora possano dar luogo ad un vantaggio competitivo per il loro valore economico, anche il software e l'algoritmo possono essere considerati know how.

Tale patrimonio di conoscenze è un asset competitivo di grande importanza per ogni azienda e, sia che lo si sfrutti attraverso accordi di trasferimento tecnologico sia che lo si usi all'interno dell'azienda per produrre un determinato prodotto/servizio, rappresenta uno degli elementi in grado di assicurare all'azienda un consistente e duraturo vantaggio competitivo sul mercato. Quindi, al pari degli altri diritti di proprietà industriale, quali marchi, brevetti e design, anche il know how detenuto da un'impresa contribuisce in maniera considerevole alla determinazione del suo valore e del suo patrimonio.

Tuttavia, per essere considerati segreti commerciali e per ricevere la tutela prevista dal CPI è necessario che sia il software che l'algoritmo siano appunto segreti; l'azienda pertanto dovrà adottare tutte le misure necessarie per mantenerli riservati.

È infatti fondamentale per l'azienda identificare con precisione quali informazioni, codici sorgente e algoritmi sono da ritenersi segreti commerciali ed industriali e stipulare con i propri dipendenti e collaboratori, ma anche con i propri fornitori e partners commerciali, accordi di riservatezza ad hoc precisi e circostanziati, evitando l'utilizzo di generici non disclosure agreement.

In generale, ogni dipendente con accesso al software o all'algoritmo dovrà firmare un apposito accordo di riservatezza.

Ugualmente, qualora il software e l'algoritmo vengano condivisi con terze parti in ragione di un determinato rapporto, dovranno essere sottoscritti anche con tali terze parti specifici accordi di riservatezza.

Le aziende, soprattutto quelle di grandi dimensioni, dovrebbero valutare chi ha davvero bisogno di avere una conoscenza diretta dell'algoritmo e del codice sorgente e concederne l'accesso solo a questi.

Oltre a questi accorgimenti di tipo contrattuale, l'impresa dovrà adottare anche misure tecnico-informatiche (es. criptazione del software) e organizzative (es. adozione di specifiche policy aziendali) idonee a tutelare la riservatezza dei segreti commerciali. Tali misure dovranno essere documentate, con lo scopo non solo di evitare la divulgazione o la sottrazione delle informazioni riservate, ma anche di permettere all'impresa di documentare quali azioni sono state messe in campo per mantenere la segretezza e rendere evidente a coloro che con esse vengono in contatto la loro natura segreta, dando la prova al giudice della violazione avvenuta.

In un eventuale giudizio, l'imprenditore dovrà di fatto dare la prova di avere in primis identificato i propri trade secrets e poi di avere adottato tutte le misure tecniche, ma anche organizzative e contrattuali idonee a tutelarli[26].

[26] Cnf. https://www.studiolegalestefanelli.it/it/approfondimenti/cosa-sono-i-segreti-commerciali-quali-le-tutele-possibili/

CAPITOLO 3 - L'INTELLIGENZA ARTIFICIALE *a cura di Laura Fragapane*

https://www.analyticsinsight.net/whats-the-difference-between-ai-and-computer-vision/

3.1 Cos'è e cenni storici

Uno dei creatori dell'Intelligenza Artificiale, Marvin Minsky afferma "*Premesso che non credo alle definizioni, direi che l'intelligenza artificiale è rappresentata da una gran quantità di persone che cercano di realizzare macchine più intelligenti e di formulare teorie sul funzionamento della mente umana. Si avvicina molto alla psicologia, solo che impiega i computer per la sperimentazione*" e nel suo libro "Semantic Information Processing", definisce la AI come "*la scienza di far fare alle macchine delle cose che richiederebbero l'intelligenza umana*".[27]

Filippo Donati definisce la AI come la "*tecnologia che permette ad un computer di analizzare grandi quantità di dati e, sulla base della conoscenza e dell'esperienza acquisita, adottare comportamenti intelligenti o proporre decisioni*".[28]

[27] Sematinc Information Processing, Marvin Minsky
https://www.repubblica.it/online/tecnologie_internet/minsky/intervista/intervista.html

[28] Filippo Donati, articolo "Intelligenza Artificiale e giustizia" Rivista AIC, 2020 https://www.rivistaaic.it/it/rivista/ultimi-contributi-pubblicati/filippo-donati/intelligenza-artificiale-e-giustizia

L'intelligenza artificiale dovrebbe quindi compiere in maniera razionale la modalità di scelta della mente umana, grazie all'uso della logica, risolvendo funzioni cognitive, ottenendo il miglior risultato atteso sulla base delle informazioni a disposizione.

Peter Norvig e Stuart Russel in "Artificial Intelligence – A modern Approach" si interrogano sulla definizione di intelligenza artificiale e concludono che le definizioni siano varie, ma raggruppabili in quattro categorie, suddivise per risultato finale simile a quello realizzato dall'uomo, o uso della razionalità.

	Fedeltà alla performance umana	**Uso della razionalità**
Focus sul pensiero	**Sistemi che pensano come esseri umani** "L'eccitante, nuovo tentativo di far sì che i computer arrivino a pensare ... Macchine dotate di mente, nel pieno senso della parola" (Haugeland, 1985) "[L'automazione delle] attività che associamo al pensiero umano, come il processo decisionale, la risoluzione di problemi, l'apprendimento …" (Bellman, 1978)	**Sistemi che pensano razionalmente** "Lo studio delle facoltà mentali attraverso l'uso di modelli computazionali" (Cherniak e McDermott, 1985) "Lo studio dei processi di calcolo che rendono possibile percepire, ragionare ed agire" (Winston, 1992)
Focus sull'azione	**Sistemi che agiscono come esseri umani** "L'arte di creare macchine che eseguono attività che richiedono intelligenza, quando vengono svolte da persone". (Kurzweil, 1990) "Lo studio di come far eseguire ai computer le attività in cui, al momento, le persone sono più brave". (Rich e Knight, 1991)	**Sistemi che agiscono razionalmente** "L'intelligenza computazionale è lo studio della progettazione di agenti intelligenti" (Poole et al., 1998) "L'IA … riguarda il comportamento intelligente negli artefatti" (Nilsson, 1998)

Negli studi del AI, tutti i quattro approcci sono stati adottati ed analizzati, concludendo che la metodologia che si è dimostrata maggiormente efficace è l'ultima: "Sistemi che agiscono razionalmente". I razionali di tale conclusione sono che, essendo in dubbio che una macchina possa pensare, la parte che si concentra sul pensiero potrebbe risultare inefficace. Inoltre, si ottiene un'efficienza quando le macchine svolgono operazioni più rapidamente dell'essere umano, che ci porta ad escludere la parte sinistra della nostra tabella.[29]

Alan Turing nel suo articolo "*Computing machinery and intelligence*" del 1950 pubblicato sulla Rivista Mind, si interroga sulla capacità di una macchina di pensare, nasce così il test di Turing, ovvero una variazione del "gioco dell'imitazione", che definisce che una macchina applica l'intelligenza artificiale se un essere umano dopo 5 minuti non è in grado di riconoscere se sta dialogando con una macchina o con un essere umano.

Molti studiosi hanno criticato il test di Turing, tra questi ricordiamo Edsger Dijkstra, che nel 1984 scrive: "*La questione se le macchine possono pensare (…) è rilevante quanto chiedersi se i sottomarini possano nuotare (…) Secondo il dizionario (…) la prima definizione di nuotare è «Muoversi in acqua attraverso gli arti, le pinne o la coda» e gran parte delle persone è d'accordo che i sottomarini, in quanto privi di arti, non possano nuotare. (…) Ma né la domanda né la risposta hanno alcuna rilevanza nella progettazione dei sottomarini (…*)".

Una delle critiche più rilevanti viene formulata da John Searle nel 1980, conosciuta come la "*stanza cinese*", sostiene che, nonostante un robot superi il test di Turing non significhi che sia in grado di rielaborare gli input circostanti adattarne gli output. Searle espone una metafora immaginando che in una stanza vi sia una singola persona, che comprende unicamente l'inglese, e un manuale in inglese e una serie di fogli in cinese. L'uomo riceve dei comandi (input) in cinese, che non comprende ma cercando tra i suoi fogli riesce a rispondere tramite delle azioni (output) non comprendendo però il cinese. Analogamente una macchina è in grado di dialogare in maniera intelligente in cinese ma non comprendendo gli input e gli output si tratta di una mera esecuzione di un programma che non comprende l'elaborazione.[30]

[29] Russell, S.J., Norvig, P, "Artificial Intelligence – A modern Approach", 3a ed., Pearson, 2010

[30] John R. Searle, "The Behavioral And Brain Sciences" (1980) 3, 417-457 e "Minds, Brains and Programs" (1980)

La macchina che agisce come se fosse intelligente è il concetto alla base dell'intelligenza artificiale debole. Semplificando, si tratta di macchine che attuano il *problem solving*, replicando alcuni ragionamenti logici umani per risolvere problemi e prendere decisioni. Un classico esempio di intelligenza debole è la macchina che gioca a scacchi.

L'intelligenza forte definita da Searle pone la macchina non come semplice strumento per lo studio della mente umana, bensì strumento a sostituzione della mente, cioè una macchina che può capire gli stati cognitivi.

Tale ipotesi viene spiegata da Putnam con la teoria del "cervello nella vasca", sostenendo che, per essere in grado di fare rifermento a qualcosa, bisogna averne una percezione diretta, chiamata "nesso causale".[31]

Con la teoria del cervello nella vasca, Putnam rivolge una critica e scredita "le teorie magiche del significato", in favore della "Teoria del riferimento".

https://laricerca.loescher.it/cervelli-morali/

Una macchina con intelligenza artificiale forte è in grado di auto-apprendere. Tipici di questa categoria sono, pertanto, i prodotti che usano processi di machine learning.

3.2. Il flusso che regola l'Intelligenza Artificiale

La Commissione Europea definisce l'intelligenza artificiale come l'insieme dei "sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di

[31] Hilary Putnam "Reason, Truth and History" 1981

autonomia, per raggiungere specifici obiettivi".[32]

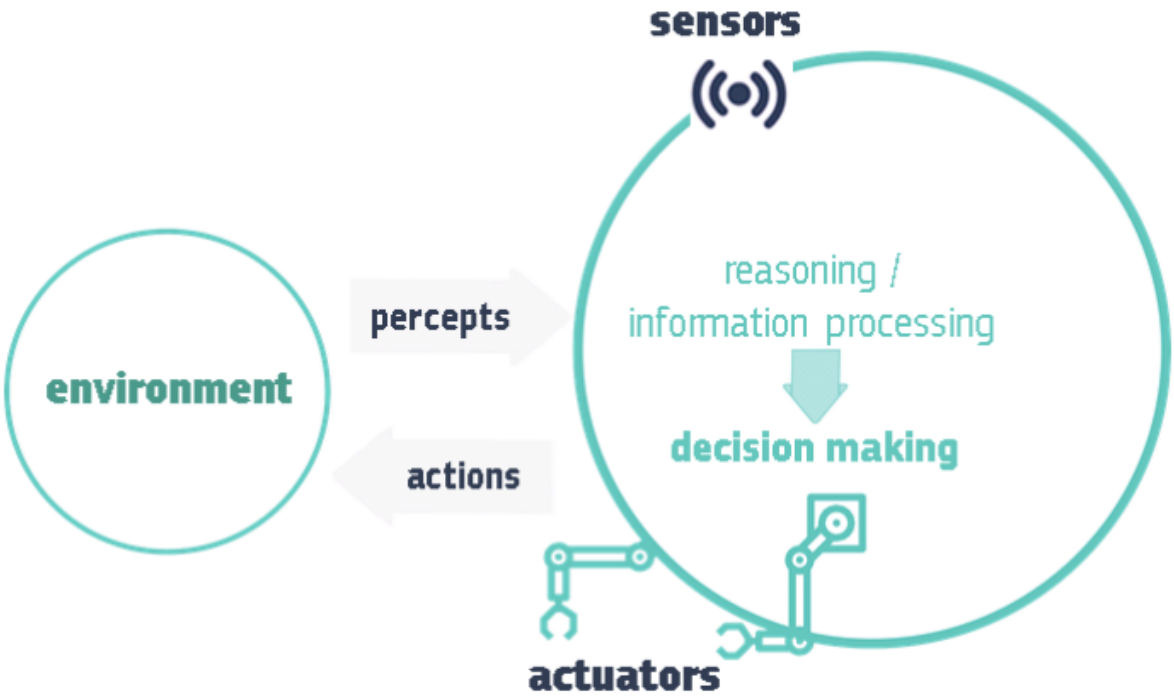


Figure 1: A schematic depiction of an AI system.

La figura sopra riportata mostra come un sistema di Intelligenza artificiale possa essere razionale in riferimento all'ambiente che lo circonda.

Infatti, l'AI percepisce l'ambiente che lo circonda tramite sensori che gli permettono di raccogliere dati ed elementi sull'ambiente circostante che analizza e da cui ne deriva il miglior risultato atteso. Le azioni intraprese dai sistemi di Intelligenza artificiale hanno un effetto sull'ambiente circostante, modificandolo.

L'AI quindi, tramite tecniche di rielaborazione dei dati e algoritmi, può adattare le proprie scelte in base a come l'ambiente muterà influenzato dalle precedenti scelte.

I sensori sono quindi fondamentali per comprendere l'ambiente circostante e rielaborare al meglio il comportamento intrapreso: essi dovranno essere trasformati in informazioni da processare.

[32] 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 on Artificial Intelligence for Europe, Brussels, 25.4.2018 COM(2018) 237 final. https://www.mise.gov.it/index.php/it/strategia-intelligenza-artificiale/contesto

Al centro del modello di intelligenza artificiale, vi è il modulo de ragionamento che elabora i dati di input derivanti dai sensori trasformandoli in informazioni e propone l'azione da intraprendere per il raggiungimento dell'obiettivo.

L'azione è eseguita dagli attuatori che, nella figura sopra, sono rappresentati da bracci robotici, ma questi potrebbero essere di diversi tipi, software, chatbot, etc.. L'azione eseguita probabilmente modificherà l'ambiente circostante, ne deriva quindi che i sensori raccoglieranno nuovi dati di input, diversi da quelli incanalati in precedenza.

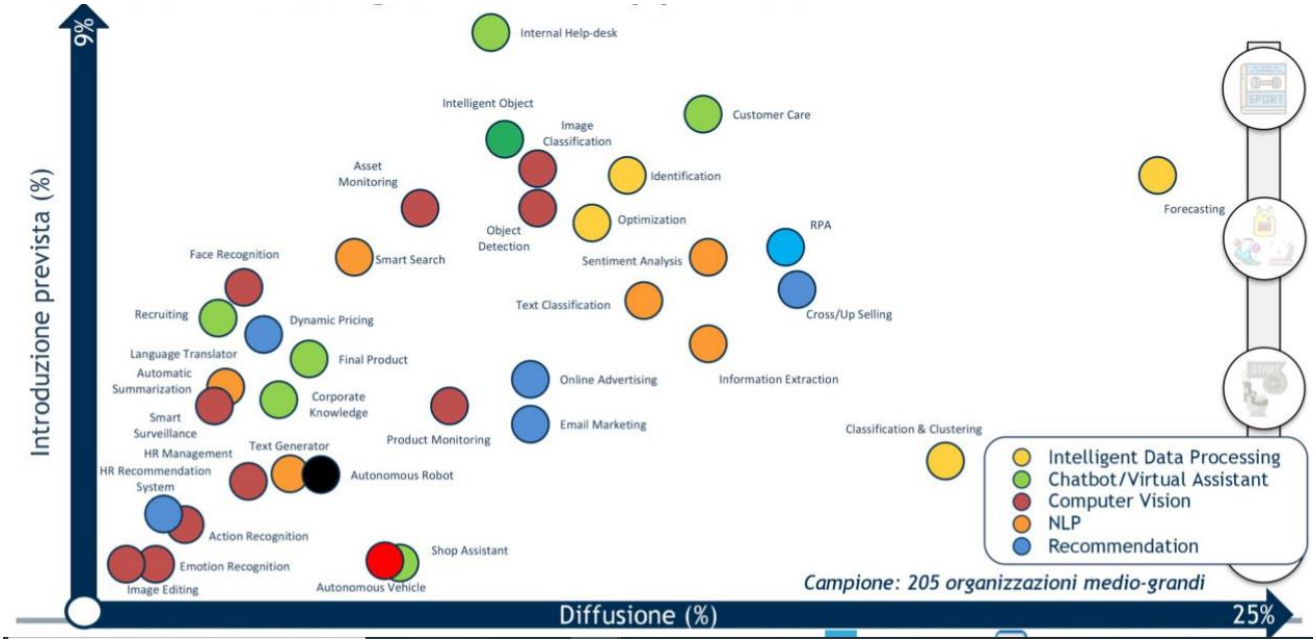
3.3 Utilizzo dell'intelligenza artificiale

L'intelligenza artificiale sta prendendo piede in moltissimi settori economici per ridurre la forza lavoro nei processi ripetitivi ma anche per rendere più efficienti i processi aziendali.

L'Osservatorio Artificial Intelligence della School of Management del Politecnico di Milano ha identificato otto classi di soluzioni di Intelligenza Artificiale attualmente esistenti:

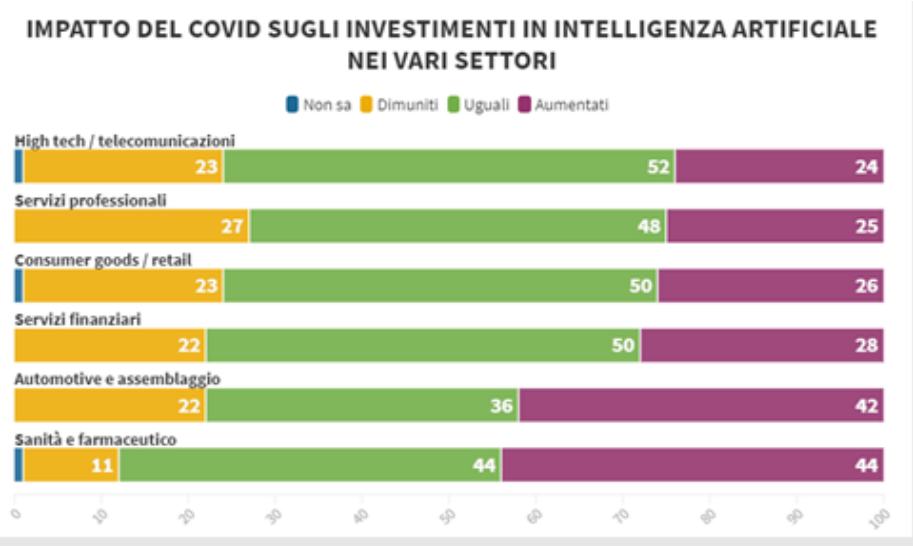
1. *Autonomous Vehicle*: mezzi di trasporto merci o persone a guida autonoma.
2. *Autonomous Robot*: robot con sembianze umane capaci di muoversi, utilizzare oggetti ed eseguire compiti senza l'iterazione umana, in grado di adattarsi all'ambiente circostante e ad eventi non previsti.
3. *Intelligent Object*: tutti gli oggetti (valige, orologi, occhiali, etc.) capaci di compiere azioni e prendere decisioni autonomamente, in grado di raccogliere input, tramite sensori, dall'ambiente.
4. *Virtual Assistant e Chatbot*: assistenti virtuali in grado di memorizzare e riutilizzare le informazioni raccolte, dimostrando intraprendenza durante le conversazioni. Alcuni di essi sono anche in grado di riconoscere il body languageo l'intonazione vocale.
5. *Recommendation*: soluzioni in grado di indirizzare le scelte dell'utente in base alle scelte precedentemente intraprese o le preferenze ed interessi selezionati. Tali soluzioni sono folto usate nell'eCommerce per guidare il processo decisionale dell'utente.
6. *Image Processing*: sistemi capaci di analizzare immagini o video e rilevare e riconoscere persone, animali e altri elementi presenti. Tale tecnologia è spesso usata per il controllo dei locali o dalle compagnie assicurative per la valutazione degli incidenti.

7. *Language Processing*: Sistemi in grado di comprendere testi, tradurli e produrre autonomamente documenti.
8. *Intelligent Data Processing*: tutte le soluzioni che utilizzano algoritmi di intelligenza artificiale per estrarre informazioni da dati strutturati. Tra gli esempi più noti ricordiamo strumenti per le rilevazioni di frodi, per la previsione del rischio, sistemi di controllo, per la cybersecurity.



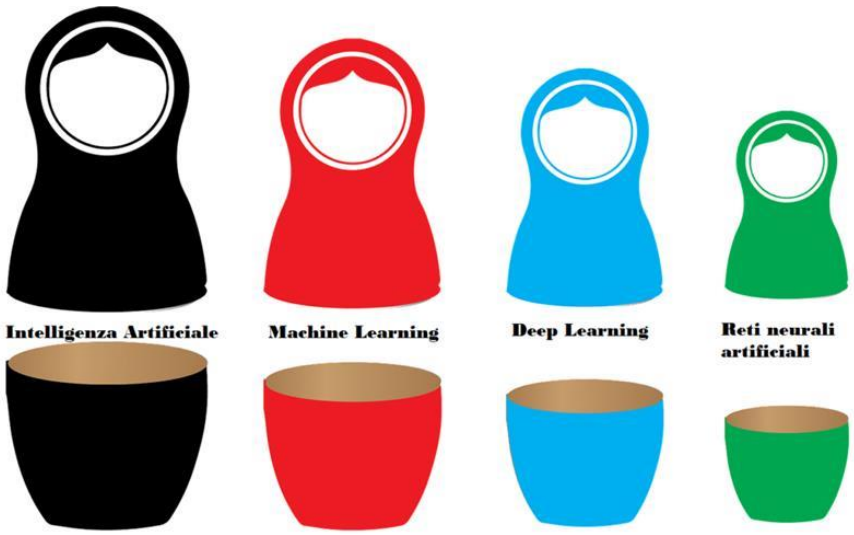
Durante la pandemia da Sars-Cov 2, grazie allo spostamento dei canali per la relazione con i clienti, il mercato dell'intelligenza artificiale non si è arrestato, anzi è cresciuto, specialmente su iniziative di Forecasting (stima della domanda), Anomaly Detection (individuazione di frodi online), Object Detection (come il riconoscimento dei DPI nelle immagini) e ancora di più di Chatbot e Virtual Assistant.[33]

[33] Alessandro Piva, Direttore dell'Osservatorio Artificial Intelligence



Fonte: McKinsey, 2020 (Valori percentuali)

CAPITOLO 4 -MACHINE LEARNING E DEEP LEARNING[34] *a cura di Fabrizia Cicero*



4.1 Machine learning e apprendimento automatico: definizione, origini e sviluppi

Il mondo dell'informatica e dell'intelligenza artificiale si è nel tempo sviluppato per dare vita a nuove differenti tecniche di apprendimento, unitamente allo sviluppo degli algoritmi creando delle interazioni che, a loro volta, consentono oggi di avere numerose possibilità di utilizzo che allargano il campo di applicazione dell'apprendimento automatico.

Il termine Machine learning viene oggi utilizzato per identificare tutti i meccanismi che permettono ad una macchina intelligente (dotata di Computer Numerical Control (CNC) e/o Programmable Logic Control (PLC) o più in generale dotata di sistemi computerizzati) di migliorare autonomamente le proprie capacità e prestazioni.

La macchina, inizialmente programmata per svolgere una determinata attività, è in grado di migliorare i propri compiti tramite l'esperienza, le proprie capacità, le risposte che rileva sul campo nell'esecuzione

[34] https://www.innovationpost.it/2021/02/18/deep-learning-che-cose-a-cosa-serve-e-perche-e-importante-nella-manifattura

dell'attività stessa. Alla base dell'apprendimento ci sono una serie di algoritmi che permettono alla macchina di prendere decisioni differenti in base all'esperienza del lavoro svolto fino a quel momento. Fra gli esempi di machine learning più comuni oggi vi sono le tecnologie di riconoscimento vocale presenti negli smartphone, gli apparecchi di domotica delle smart home e la guida autonoma delle automobili. Anche a livello di marketing e comunicazione è possibile utilizzare macchine che sfruttano l'apprendimento automatico, come nel caso dell'elaborazione di big data con machine learning, dei risultati presenti nelle SERP (Search Engine Results Page) dei motori di ricerca, dei filtri antispam delle mail e delle pubblicità personalizzate.

Le prime sperimentazioni per realizzare macchine intelligenti risalgono agli anni Cinquanta e sono state basate su specifici modelli probabilistici al fine di realizzare macchine che fossero in grado di auto apprendere in base alle probabilità di accadimento di uno specifico evento. Lo studioso Alan Turing sviluppò per primo gli algoritmi che permettessero di sviluppare macchine in grado di apprendere. I suoi studi proseguirono nell'ambito dell'intelligenza artificiale, sui sistemi esperti e sulle reti neurali; non poche furono le difficoltà di reperimento delle risorse in questo campo, poiché da parte della scienza c'era un profondo scetticismo riguardo al progetto di realizzare macchine che fossero in grado di apprendere.

Solo negli anni Ottanta il rinnovato interesse su questi progetti permise di definire un programma di investimenti tale da assicurare le risorse necessarie.

Alla fine degli anni Novanta il progetto di autoapprendimento divenne prioritario anche in considerazione dell'applicazione di nuovi modelli statistici e probabilistici; questo permise lo sviluppo che ha portato oggi all'apprendimento automatico, come ramo della ricerca pienamente riconosciuto ed altamente richiesto dal mercato.

4.2 Le modalità di apprendimento

Ad oggi esistono differenti modalità di apprendimento che differiscono fra loro per gli algoritmi utilizzati e per lo scopo per cui sono realizzate le macchine stesse. A seconda del tipo di algoritmo utilizzato per permettere l'autoapprendimento, ovvero a seconda della modalità con cui la macchina apprende e accumula dati e informazioni, si possono classificare tre principali sistemi di apprendimento:

- supervisionato;

- non supervisionato;
- per rinforzo.

L'apprendimento supervisionato consiste nel fornire al sistema informatico della macchina una serie di nozioni di base e di esempi che popoleranno inizialmente il database di informazioni ed esperienze. Quando la macchina si troverà di fronte ad un problema analizzerà le informazioni presenti nel proprio database e deciderà quale azione intraprendere in base al modello codificato.

Questo tipo di apprendimento, dotato inizialmente di un pacchetto di informazioni confezionate permette alla macchina di agire scegliendo fra le esperienze codificate e presenti nel database. Gli algoritmi che fanno uso dell'apprendimento supervisionato vengono utilizzati in molti settori dal campo medico al riconoscimento vocale; per mezzo quindi di ipotesi induttive, ovvero ipotesi che possono essere ricavate dalla macchina analizzando il proprio database, è possibile arrivare alla soluzione del problema che si pone.

Ovviamente più è ricco il database preconfezionato fornito alla macchina maggiore sarà la probabilità per la macchina stessa di trovare la soluzione. Ad esempio, questo tipo di apprendimento viene usato soprattutto per problemi di classificazione: un esempio di applicazione sono i sistemi antispam delle e-mail. Infatti, all'arrivo di una nuova e-mail, il sistema riesce a decidere se questa debba essere etichettata come spam o meno.

L'apprendimento non supervisionato prevede che le informazioni inserite all'interno del database della macchina non siano codificate, ossia la macchina può attingere a tali informazioni ma non ci sarà alcun esempio del loro utilizzo e quindi non conoscerà il risultato atteso a seconda della scelta individuata. Sarà quindi compito della macchina catalogare tutte le informazioni in suo possesso, organizzarle, impararne il significato, l'utilizzo e il risultato a cui portano in base alla scelta effettuata.

Tale apprendimento offre a bene vedere maggiore libertà di scelta alla macchina che dovrà utilizzarle con "intelligenza" imparando quale sia il risultato migliore per le differenti situazioni che si presentano. È spesso utilizzato nelle discipline mediche o di biologia per l'analisi diagnostica o per l'individuazione di gruppi genetici; inoltre, trova grande applicazione oggi nell'ambito dei Big-Data quando è necessario correlare diversi dati ed estrarre informazioni non note.

L'apprendimento per rinforzo è, infine, il più complesso; prevede infatti che la macchina sia dotata di sistemi e strumenti che le consentano di migliorare il proprio apprendimento e di comprendere le caratteristiche dell'ambiente di contesto.

A tale scopo, nella macchina vengono installate specifiche apparecchiature quali telecamere, sistemi GPS etc. che permetteranno di rilevare il contesto ed effettuare la scelta appropriata per il proprio adeguamento alle varie situazioni.

Nei progetti di auto con guida autonoma, ad esempio, vengono analizzati ed elaborati una serie di dati raccolti dall'auto durante il suo percorso: il tipo di strada che si sta percorrendo, la segnaletica, le condizioni ambientali, il traffico intorno e il percorso programmato. In base all'elaborazione dei dati l'auto procederà nel suo percorso in condizioni di sicurezza, ma sarà pronta a cedere il controllo al pilota appena questi azionerà i comandi manualmente. Questo tipo di apprendimento è utilizzato frequentemente nella robotica, per controllare i movimenti degli automi, e anche in ambiti industriali nella produzione e nel controllo qualità.

4.3 Il Machine learning ed estrazione dei dati: il Data-mining

Una delle principali caratteristiche del machine learning è la sua stretta correlazione con altri rami dell'informatica, della statistica, dell'ottimizzazione e di molti altri settori delle moderne scienze intelligenti. L'interrelazione fra questi diversi rami è fondamentale per poter realizzare strutture in grado di risolvere i più differenti problemi che permettono ad una macchina di apprendere secondo le tre differenti modalità tipiche dell'apprendimento intelligente.

Ad esempio, quando si parla di data mining, ovvero delle tecniche e metodologie che hanno per oggetto l'estrazione di informazione da grandi quantità di dati, si parla sempre di una forma di apprendimento, ma limitata al solo apprendimento non supervisionato. Il data mining, infatti, punta all'estrazione di informazioni e dati per il miglioramento delle conoscenze della macchina; esso punta esclusivamente ad incrementare la quantità di informazioni disponibili contribuendo al miglioramento della macchina tramite conoscenze sempre nuove.

Il machine learning invece ha come scopo quello di un apprendimento sempre più profondo, che partendo dalla disponibilità di nuove conoscenze, si propone di riprodurre tali conoscenze, con lo scopo di un miglioramento sempre più avanzato della macchina per utilizzi sempre più specifici. Similmente, anche con altri rami della ricerca del machine learning si possono avere sovrapposizioni di metodologie e risultati. Tra questi, ad esempio, vi è l'ottimizzazione, ossia il miglioramento dell'efficienza del sistema che permette di ottenere risultati in maniera più rapida e meno dispersiva.

Le possibilità di sviluppo futuro di questo ramo sono comunque ancora molte, soprattutto sono legate a diversi settori di applicazione, non solo scientifici e legati alla ricerca, ma anche di uso comune.
La domotica ha già fatto uso di alcuni dei più semplici sistemi di apprendimento automatico, la disponibilità commerciale di apparecchiature che colloquiano con l'utente al fine di gestire l'ambiente domestico ne sono un esempio: Amazon Alexa, Microsoft Cortana, Apple Siri, Google Home etc..
Scopo della ricerca è quindi integrare la vita quotidiana e i processi industriali più specifici con strumenti che siano di aiuto nell'esecuzione di attività che fino ad oggi necessitano dell'uomo.
La disponibilità di un immenso patrimonio di dati ed informazioni costituisce la base per affinare algoritmi e tecniche di analisi che permetteranno alle macchine, ai PC, alla Domotica di fornirci un aiuto sempre più qualificato ed efficace.

4.4 I rischi legali e profili di responsabilità

Occorre infine esaminare una prima classificazione dei rischi legali, riferibili allo sviluppo di metodologie e tecnologie di intelligenza artificiale e del machine learning comprendenti i rischi "determinati dalla causalità" e rischi "determinati dai dati".
Per rischi "determinati dalla causalità" ci si riferisce al modo in cui si decidono, a oggi, le questioni relative all'imputazione della responsabilità umana che, come è noto, si basa - secondo la tradizione giuridica - sull'attribuzione delle conseguenze fattuali di una condizione soggettiva, colpa o dolo, a un essere umano, individuato per il tramite dell'applicazione del principio di causalità che richiede l'applicabilità di una legge scientifica di copertura, idonea, secondo i suoi precetti, a ricondurre secondo un rapporto di causa/effetto un evento alla sua causa. Se è possibile individuare la causa o il difetto, per esempio, di un'attività di elaborazione elettronica, sarà possibile anche individuare la responsabilità per il danno e quindi la colpa che insieme hanno causato il danno. L'intensità della colpa, una volta identificata, determina la severità della pena e/o le altre modalità di compensazione del danno causato.
Il limite dell'applicazione dei principi della causalità naturale a fenomeni correlati a processi decisionali algoritmici di machine learning - e quindi il relativo rischio di errore nella valutazione della corrispondente responsabilità - risiede, principalmente nel fatto che il soggetto che apprende non è un essere umano, e pertanto le decisioni che esso adotta o gli atti che compie possono essere molto lontane da qualsiasi logica implementata dall'essere umano nel codice software della macchina.

Nello scenario descritto viene quindi a mancare, o quanto meno viene molto attenuato, il nesso diretto tra codice software e comportamento del sistema di elaborazione, che è invece alla base dell'attribuzione della responsabilità del produttore nell'attuale scenario giuridico. Ciò, in quanto la disciplina dell'attribuzione della responsabilità nasce all'interno di un quadro giuridico di tracciabilità diretta dei difetti. Cioè le decisioni e gli atti delle macchine dovrebbero poter essere ricondotti a uno specifico difetto nella programmazione ovvero all'esecuzione di un'operazione incorretta. Un riferimento normativo utile alla comprensione dell'estrema delicatezza e rilevanza sociale, oltre che economica, delle questioni implicate dalle tematiche relative all'uso del machine learning, può rinvenirsi, oltre che naturalmente nelle disposizioni del Regolamento Generale in materia di protezione dei dati personali (di seguito anche denominato "GDPR"), anche nella direttiva n. 680 del 27 aprile 2016, in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

In particolare, l'art. 11 della direttiva richiamata indica come il processo decisionale automatizzato relativo alle persone fisiche, preveda che gli Stati membri dispongano che una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici negativi o incida significativamente sull'interessato, sia vietata salvo che sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento. Inoltre, deve prevedere garanzie adeguate per i diritti e le libertà dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento.

Se i rischi determinati dalla causalità di cui abbiamo sin qui trattato possono essere definiti rischi "esterni", nel senso di comportare implicazioni in virtù dell'applicazione di regole giuridiche esterne a quelle del sistema di machine learning, quelli "determinati dai dati" - specialmente dai big data – possono essere definiti rischi 'interni' al sistema stesso.

I big data pongono un problema in cui si accavallano il modo con cui le aziende capitalizzano il flusso di terabyte di dati generati in modalità "smart streaming" dai dispositivi "intelligenti" e la disponibilità di modelli e algoritmi di machine learning di analisi predittiva che stanno trasformando il modo in cui le aziende si riferiscono ai loro clienti e che generano da sé questioni controverse oltre a costituire fattori di rischio per la privacy e la protezione dei dati personali.

Lo smart streaming dei dati è stato già più volte oggetto dell'attenzione del legislatore e dei regolatori. La Commissione Europea, a tal proposito, ha pubblicato la propria "Strategy on Co-Operative Intelligent Transport Systems" o "CITS" per lo sviluppo di un'infrastruttura intelligente di trasporto che permetta agli autoveicoli di comunicare tra di loro e con un sistema centralizzato di gestione del traffico, nonché con altri agenti del sistema di trasporto.

Il rischio potenziale di utilizzo improprio di dati è chiaramente dovuto al fatto che l'infrastruttura è capace di identificare ogni singolo veicolo in tempo reale lungo il suo percorso, conoscerne la destinazione, riportare il comportamento del conducente e ogni eventuale infrazione alle norme di circolazione, con evidente conoscenza di informazioni anche relativa a dati personali dei soggetti utilizzatori.

4.5 Il Deep Learning: definizione e origini

Il termine Deep Learning significa letteralmente "apprendimento approfondito" e la funzione che svolge il deep learning è proprio quelli di creare modelli di apprendimento su più livelli. A livello esemplificativo, potremmo prendere a riferimento una nozione, che una volta appresa, lascia il posto ad un altro concetto. La mente umana recepisce l'input della prima nozione appresa e la elabora insieme alla seconda, trasformandola e astraendola sempre di più.

A livello scientifico, l'azione del deep learning consiste nell'apprendimento di dati non trasmessi dall'uomo, ma appresi grazie all'utilizzo di algoritmi di calcolo statistico. Lo scopo di questi algoritmi è comprendere il funzionamento del cervello umano e come questo riesca ad interpretare le immagini e il diverso linguaggio. L'apprendimento così realizzato si potrebbe rappresentare come una sorta di una piramide, dove, all'apice vi sono i concetti più alti che vengono appresi partendo dall'apprendimento dai livelli più bassi.

Il deep learning ha conosciuto nell'ultimo decennio uno sviluppo enorme, ottenendo risultati che, fino a qualche tempo fa, erano impensabili. Tale successo è dovuto alle numerose scoperte ed innovazioni avvenute nel campo informatico, relative soprattutto alla sfera dell'hardware, con lo sviluppo di un calcolatore che riesce a fare esperienza su un quantitativo sempre maggiore di dati sensibili. Oggi, grazie all'introduzione delle GPUs, ovvero nuove unità che concorrono all'elaborazione dati, questo processo si è semplificato.

Un altro importante sostegno allo sviluppo di forme di deep learning è derivato dalla facilità di trovare numerose collezioni di dati ("dataset") fondamentali per allenare il sistema. Il deep learning, infatti, fornisce una rappresentazione dei dati a livello gerarchico e soprattutto fornendo una panoramica di tutte le nozioni diverse tra loro, riuscendo a elaborarle e a trasformarle. La macchina riesce quindi a classificare i dati in entrata ("input") e quelli in uscita ("output"), evidenziando quelli più rilevanti ai fini della risoluzione del problema e scartando quelli che non necessari. La rivoluzione apportata dal deep learning consiste nella capacità, simile a quella umana, di elaborare i dati, le proprie conoscenze anche a più a livelli e grazie a questa facoltà la macchina apprende e perfeziona funzionalità sempre più complesse.

Nel 1958 lo psicologo Rosemblatt presentò al mondo accademico il famoso Perceptron, una rete neurale artificiale, alimentata da un computer che aveva le stesse dimensioni di una stanza. L'evento suscitò enorme entusiasmo nei media poiché Perceptron, era riuscito a distinguere, dopo 50 tentativi, alcune tessere contrassegnate a destra da quelle a sinistra. A causa dei limiti di una rete neurale artificiale composta da un solo strato di neuroni, Perceptron fu poi archiviato, non senza aver dato una spinta innovativa alla ricerca e aiutandola a fare grandi passi in avanti. Il prototipo di macchina intelligente di Rosemblatt riprese vigore nei primi anni Ottanta grazie agli scienziati informatici Hinton e LeCun, i quali pubblicarono uno studio attraverso il quale veniva proposto un percorso per insegnare alle reti neurali a correggere gli errori. La tecnologia non era però ancora abbastanza evoluta per permettere di vedere dei miglioramenti. Solo nei tempi moderni vi sono stati sviluppi significativi di tale utilizzo delle macchine grazie anche all'intervento di big player del settore dell'informatica, che hanno iniziato ad inserire il deep learning nei propri programmi commerciali.

4.6 Il successo del Deep learning

Nel 2021, anno fondamentale per lo sviluppo del deep learning, sono stati presentati gli straordinari risultati ottenuti in un esperimento condotto dal professor Hinton a Toronto, durante il contest ImageNet. L'esperimento era volto al riconoscimento visivo, effettuato tramite software prova (benchmark), in un settore fino ad allora arduo e mai esplorato: la capacità di distinguere 1000 categorie visive. Lo scienziato, in un colpo solo, ottenne un miglioramento epocale: il 10% in una volta sola. Nel corso di questo esperimento, il pool di studiosi presentò questa nuova tecnologia che aveva

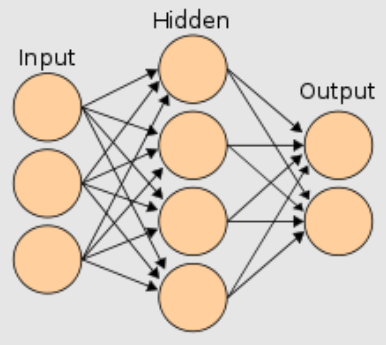
consentito alla macchina di riconoscere uomini e animali tramite il confronto con milioni di altre immagini, senza il bisogno di un intervento codificato da parte dell'uomo.

Il sistema Imagenet è stato poi utilizzato nel 2015 per presentare i clamorosi risultati di una ricerca incredibile. Il pool di scienziati riuscì a creare un deep learning su 152 livelli di astrazione, a confronto dei soli 30 livelli di astrazione fino ad ora esplorati.

Da ciò si comprende facilmente che più sono i livelli di astrazione, più la macchina ha una notevole capacità di apprendimento, mostrandosi più intelligente.

Le reti neurali sono alla base dello sviluppo del deep learning. Per meglio comprenderne il concetto, occorre analizzare come nell'annosa diatriba relativa alla supremazia tra intelligenza artificiale debole e forte, abbiamo visto come si sia insinuato un nuovo ed elaborato concetto. Una macchina potrà definirsi veramente intelligente solo quando sarà in grado di riprodurre un sistema di ragionamento che sia biologicamente ispirato al cervello dell'uomo, offrendo cioè un sistema di ragionamento, simile al funzionamento dei neuroni umani.

Di seguito, un esempio di sviluppo delle reti neurali artificiali[35]:



Anche nel mondo del deep learning, così come per l'essere umano, il neurone ha un'importanza fondamentale.

Il neurone umano è lo strumento che occorre per nutrire il deep learning attraverso le famose Reti Neurali Artificiali. Una rete neurale, infatti, cerca di riprodurre il funzionamento del neurone umano, ovvero tutti quei processi che avvengono nel cervello durante la fase di apprendimento e quella successiva del riconoscimento.

[35] https://www.intelligenzaartificiale.it/deep-learning/

Nel processo di apprendimento la pura e semplice esperienza guida l'apprendimento e offre al cervello i dati necessari per comprendere.

Nei software "neuronali" il processo umano di apprendimento viene sostituito dall'azione di un programmatore che immette dei dati conosciuti nella macchina ed inserisce così i parametri di riferimento di quel neurone per ottenere quel preciso risultato. In tal modo il programmatore inserisce l'esperienza nella macchina in modo tale da consentirle di rispondere in modo corretto anche quando si troverà davanti dei dati totalmente nuovi.

La rete neurale quindi apprende grazie all'esperienza, legge i dati, costruendo architetture gerarchiche e fornendo livelli avanzati di input-output senza una vera programmazione alla base ma con un sistema di addestramento.

Nel campo della "visione artificiale" il deep learning ha fatto passi da gigante offrendo oggi un PC che comprende, in maniera del tutto automatica, un'immagine e riconosce tutti gli elementi che fanno parte di essa. Il computer, quindi, guarda e osserva il mondo circostante esattamente come l'uomo.

E se il concetto della "computer vision" può sembrare ancora un'entità astratta, basta dare un'occhiata alla realtà nella quale viviamo per accorgerci che la visione artificiale fa parte del nostro quotidiano. Sistemi di media communication come Twitter hanno la capacità di riconoscere le immagini pornografiche, eliminandole all'istante, senza la necessità di un supervisore umano. Google, nella sezione dedicata alle foto, cataloga le immagina, inserendole nelle categorie adatte. Oppure Facebook con la capacità di riconoscere i visi e taggarli dimostra come la computer vision sia a tutti gli effetti nella nostra realtà quotidiana, anche quando non ce ne accorgiamo.

Un campo dove l'utilizzo del deep learning può dare risultati importanti è senza dubbio quello della diagnostica medica. L'applicazione del concetto delle reti neurali in tale ambito è molto semplice perché i medici, molto spesso, si servono già degli algoritmi, soprattutto in ambito specialistico: l'applicazione dell'apprendimento approfondito spazia con successo dai programmi finalizzati alla diagnostica medica fino al controllo di qualità nelle produzioni farmaceutiche.

Un altro campo affascinante relativo alla possibile applicazione del deep learning è quello relativo alla guida automatica. La guida automatica consente di riconoscere gli ostacoli in entrambi i lati della carreggiata, grazie all'ausilio di sensori e telecamere in grado di elaborare le immagini.

La computer vision in questo caso riproduce la vista umana, riconoscendo l'ambito nel quale si sta muovendo e fornendo tutte le indicazioni utili per muoversi in sicurezza. L'innovazione che ha

consentito la realizzazione di automobili automatiche è stata dal deep learning, essendo ora in grado di elaborare ben 20 miliardi di operazioni al secondo.

4.7 Il futuro del Deep learning

Il futuro del deep learning prevede di poter offrire all'uomo la capacità di essere compreso dalla macchina, attraverso la comprensione del linguaggio orale e dei gesti. Lo studio e lo sviluppo degli algoritmi intelligenti saranno sempre più finalizzati alla creazione di macchine pensanti, con le quali poter interagire senza bisogno di altre interazioni e che serviranno a semplificare la vita di tutti i giorni. La ricerca sta studiando modelli che possano consentire alla macchina di comprendere i processi cerebrali dell'uomo, fino ad arrivare addirittura alla possibile comprensione del pensiero umano e dello stato d'animo.

Si tratta come chiaro di una svolta epocale: il deep learning ed il machine learning rappresentano il futuro e l'intelligenza artificiale il contesto del quale non si potrà più fare a meno. Anche se ancora numerosi sono gli step necessari al raggiungimento dei vari obiettivi, si può ragionevolmente affermare che l'apprendimento approfondito non potrà far altro che apportare numerose migliorie e benefici nella vita di tutti. Dal microcosmo individuale al macrocosmo delle industrie, l'automazione intelligente diventerà sempre più uno strumento fondamentale per gestire e rendere più semplice e intuitiva l'interazione umana con la realtà che lo circonda.

4.8 Applicazione del machine learning o deep learning nel mondo dell'energia

L'intelligenza artificiale e tutti i suoi sviluppi, a partire dal machine learning, stanno avendo già da diversi anni un impatto profondo anche nel settore elettrico.

Esistono molteplici esempi di applicazioni e attività di ricerca, tra cui ad esempio la possibilità di prevedere guasti e assicurare una manutenzione dinamica: una start-up britannica (Verv) ha sviluppato ad esempio uno smart meter che usa algoritmi di AI per predire guasti dei singoli elettrodomestici ed evitare così guasti improvvisi e ridurre i costi di manutenzione intervenendo in anticipo, capace inoltre di segnalare i dispositivi siano stati rimasti accesi in maniera accidentale

Nel campo dell'efficienza energetica, spicca la società Deepmind, parte del colosso Google, che nel 2016 ha utilizzato l'AI per ridurre l'uso di energia elettrica nei data centre Google ed ottenere un

risparmio del 40% dei costi di raffreddamento delle macchine. Il modello è stato "istruito" con anni di dati operativi storici per poi definire modalità di utilizzo e consumo i singoli server specifici.

Nel campo poi della produzione rinnovabile la società DeepMind ha sviluppato un algoritmo basato su reti neurali "istruite" con un database di dati meteo e dati storici su turbine eoliche per fornire una stima previsionale dell'output di un impianto eolico da 700 MW con 36 ore di anticipo e consentire l'ottimizzazione del dispacciamento e della consegna alla rete elettrica con 24 ore di anticipo[36]. Ciò ha di fatto aumentato del 20% il valore dell'energia elettrica prodotta dagli impianti eolici[37].

Un recente studio della Commissione Europea[38] ha poi evidenziato come l'AI avrebbe il potenziale di ridurre del 10% l'uso di energia elettrica usando il Deep Learning per predire la domanda e la produzione di energia elettrica, come anche il machine learning contribuirebbe a determinare un risparmio del 12% sul consumo di carburante per i voli aerei commerciali attraverso l'ottimizzazione delle rotte (scegliendo ad esempio rotte in cui si prevede vi siano condizioni di vento più favorevoli). Esistono tuttavia diverse criticità e ancora molti interrogativi legati allo sviluppo dell'AI e al suo utilizzo. Tra questi, ad esempio, la circostanza per cui i modelli di machine learning si basano sulla disponibilità e sulla qualità dei dati a disposizione senza considerare che se, ad esempio, i dati sono sbagliati (o anche alterati in maniera volontaria attraverso attacchi informatici) questo porterebbe ad un output errato e potrebbe esserne difficile il rilevamento del fatto che lo stesso sia errato. Tale problema avrebbe numerose ripercussioni negative se ad esempio l'AI venisse utilizzata per applicazioni "safety-critical" come la gestione di alcuni impianti di produzione elettrica o il dispacciamento dell'energia sulla rete elettrica. Inoltre, molti modelli di AI sono essenzialmente delle "black-box", cioè sistemi in cui l'utente ha normalmente visione degli input e degli output ma non dell'algoritmo e di come gli output vengano ottenuti (anche per via della loro complessità): questo potrebbe determinare una mancanza di trasparenza, come anche la difficoltà di rinvenire oggi dei riferimenti normativi legati alle tecnologie AI determinati essendo tutta le regolazione ancora agli inizi ed il suo quadro regolatorio in fase di sviluppo.

[36] DeepMind, "DeepMind AI Reduces Google Data Centre Cooling Bill by 40%", 2016
[37] Sito della società DeepMind (parte di Google), "Machine learning can boost the value of wind energy", 2019
[38] Commissione Europea, "USA-China-EU plans for AI: where do we stand?", 2018.

Numerosi sono poi i problemi etici che potrebbero sorgere in virtù dell'utilizzo dell'AI, ad esempio, per la gestione di situazioni di pericolo per la vita umana (come in caso di incidenti ed eventi non previsti su impianti e reti elettriche): difatti l'AI potrebbe decidere di agire in maniera diversa rispetto alla sensibilità di un essere umano. Tra gli esempi più noti che può essere trasposto anche al settore elettrico è quello già menzionato dell'auto a guida autonoma.

In definitiva, l'AI e le tecnologie ad essa connesse (come Machine Learning e Deep Learning) hanno, e avranno sempre più, un impatto globale e duraturo su tutti gli aspetti della società, incluso il settore elettrico. Lo sviluppo tecnologico sta già affrontando alcune delle fragilità tecnologiche grazie ad algoritmi AI sempre più robusti contro le situazioni impreviste e gli attacchi informatici. Tuttavia, l'effettivo sviluppo dipenderà anche dalla definizione di un quadro regolatorio chiaro ed equilibrato che consenta di affrontare e superare gli interrogativi di trasparenza/affidabilità ed etici che accompagnano l'Intelligenza Artificiale attualmente.

CAPITOLO 5 - PROTEZIONE GIUDICA DELL' INTELLIGENZA ARTIFICIALE: LIMITI E DUBBI *a cura di Federica Saraceni e Sabrina Panfili*

https://www.dirittodellinformatica.it/intelligenza-artificiale/cosa-cambia-con-la-nuova-proposta-ue-sullintelligenza-artificiale.html

5.1 Il nuovo approccio europeo all'Intelligenza Artificiale[39]

La protezione giuridica dell'AI, nell'ambito dell'Intellectual Property, trova il suo limite nella necessità di perseguire un delicato e armonico equilibrio tra esigenze di tutela dei diritti fondamentali dell'uomo e l'esigenza di favorire innovazione e sviluppo tecnologico, preservando la centralità della persona rispetto alla macchina e allo stesso tempo di creando fiducia sull'impiego dell'intelligenza artificiale.

[39] Fonti utilizzate ai fini della stesura del Capitolo 5 (Par. 5.1, 5.2,5.3,5.4):

- www.filodiritto.com: "Il nuovo Regolamento sull'Intelligenza Artificiale: perché, com'è e quanto costa" Avv. di Roberto Louhichi – Articolo pubblicato il 07 Maggio 2021;
- www.altalex.com: "Intelligenza Artificiale, il nuovo quadro normativo europeo" Articolo di Claudio Palmieri pubblicato il 18 Agosto 2021;
- www.agendadigitale.eu: "Intelligenza artificiale e proprietà intellettuale: come promuovere innovazione e certezza del diritto" Articolo di Marco Martorana e Roberta Savella, pubblicato il 12 Marzo 2021
- www.buignon.eu: "QUANDO L'INTELLIGENZA ARTIFICIALE INVENTA O CREA" Articolo di Simone Milli pubblicato in Bugnion News n.40 (Marzo 2020)
- www.quotidianogiuridico.it: "Responsabilità civile, etica e tutela dei diritti di proprietà intellettuale nei sistemi di intelligenza artificiale" articolo di Vanessa Cocca, pubblicato il 13 aprile 2021
- www.e-lex.it: Intelligenza artificiale e titolarità dei brevetti: a proposito di una recente decisione inglese" articolo di Giovanni Maria Riccio pubblicato il 28 Settembre 2020 ;

Il nuovo approccio dell'Unione Europea in materia di AI comprende una proposta di regolamento pubblicata il 21 Aprile 2021 (che stabilisce i requisiti di sicurezza dei prodotti, che sostituendo l'attuale "Direttiva Macchine" n. 2006/42/CE) e fa seguito ad una serie di iniziative intraprese negli ultimi anni, tra cui:

- la *Consultazione pubblica sul Libro Bianco sull'Intelligenza Artificiale* (COM 2020) 65 final del 19 febbraio 2020);
- le *Linee guida etiche finali per un'intelligenza artificiale affidabile* pubblicate l'8 aprile 2019;
- il *Rapporto sulla responsabilità per l'Intelligenza Artificiale e altre tecnologie emergenti*, pubblicato il 21 novembre 2019;
- la *Dichiarazione di cooperazione sull'intelligenza artificiale,* firmata da 25 paesi europei il 10 aprile 2018, che si basa sui risultati e sugli investimenti dell'unione à europea della ricerca e delle imprese nell'IA e stabilisce le basi per il Piano coordinato sull'IA.

5.2 La bozza di Regolamento UE sull'intelligenza artificiale

Il 21 aprile 2021 la Commissione Europea ha presentato la propria proposta di Regolamento europeo sull'Intelligenza Artificiale, volto ad introdurre una disciplina unanime e condivisa tra gli Stati Membri nell'ottica di garantire i diritti e le libertà fondamentali di tutti i cittadini europei.

Se approvato, il Regolamento introdurrà un set di obblighi particolarmente significativi relativamente ai sistemi AI, che ricalcheranno l'approccio del Regolamento europeo sulla protezione dei dati.

Nel progetto della Commissione, il Regolamento dovrebbe applicarsi praticamente a ogni soggetto appartenente alla filiera, dunque:

1. Provider dei sistemi AI;
2. Chiunque utilizzi i sistemi;
3. Produttori, importatori e distributori dei sistemi.

Al pari del Regolamento Europeo n. 679/2016 in materia di protezione dei dati personali (cd. "GDPR"), l'ambito di applicazione territoriale del Regolamento non si esaurirà ai soli soggetti stabiliti in UE, estendendosi anche a tutti coloro che, pur non essendo radicati sul territorio europeo:

- Mettono in commercio il sistema AI nell'Unione; o
- Implementano un sistema AI i cui effetti si producono sul territorio dell'Ue.

Il progetto di Regolamento classifica i prodotti che utilizzano completamente o parzialmente il software AI in base al rischio di impatto negativo su diritti fondamentali quali la dignità umana, la libertà, l'uguaglianza, la democrazia, il diritto alla non discriminazione, la protezione dei dati e, in particolare, la salute e la sicurezza.

Più il prodotto è suscettibile di mettere in pericolo questi diritti, più severe sono le misure adottate per eliminare o mitigare l'impatto negativo sui diritti fondamentali, fino a vietare quei prodotti che sono completamente incompatibili con questi diritti.

I sistemi AI vengono quindi raggruppati in vere e proprie categorie based-risk:

1. Rischio inaccettabile;
2. Rischio alto;
3. Rischio limitato;
4. Rischio minimo.

A seconda dell'appartenenza a una di queste classi, il sistema AI dovrà rispettare i relativi obblighi.

1. <u>Rischio inaccettabile</u>

I sistemi AI a rischio inaccettabile per i diritti e le libertà dei cittadini UE saranno sostanzialmente vietati.

Rientrano in questa classe:

- Sistemi AI che circonvengono il comportamento dell'utilizzatore manipolandone il comportamento. La Commissione fa l'esempio dei giocattoli con assistente vocale che incoraggino i bambini a comportamenti pericolosi.
- Sistemi AI utilizzati per individuare le vulnerabilità di uno specifico gruppo ai fini di danneggiarlo;
- Sistemi AI di social scoring "in senso stretto", ovverosia che utilizzano i dati raccolti correlati a un determinato ambito per categorizzare l'individuo in relazione a servizi riferibili ad ambito diverso

rispetto al primo. Si pensi all'utilizzo dei dati di videosorveglianza raccolti su un treno per attribuire un punteggio sociale al cittadino a cui possa poi farsi riferimento per consentire o inibirne l'accesso, ad esempio, manifestazioni sportive.

2. Rischio alto

I sistemi rientranti in questa classe verranno definiti sulla base dell'utilizzo che potrebbe esserne fatto.

Così, sono considerati sistemi AI ad alto rischio quanti verranno utilizzati in riferimento alle seguenti aree:

a) Infrastrutture critiche (ad es. trasporti) che potrebbero mettere a rischio la vita dei cittadini;

b) Sistema scolastico, che potrebbero inibire o limitare l'accesso all'istruzione (ad es. sistemi di scoring degli esami);

c) Componentistica di sicurezza dei prodotti (ad es. applicazioni per i robot di chirurgia plastica);

d) Recruiting dei candidati (ad es. sistemi AI per la scrematura dei curriculum);

e) Amministrazione della giustizia (ad es. sistemi per la valutazione delle prove);

f) Accesso a servizi essenziali (ad es. Sistemi AI per il credit rating).

L'allegato III della proposta individua aree ed utilizzi a rischio alto a cui fare riferimento e verrà aggiornato su base annuale dalla Commissione.

Tutti questi sistemi dovranno rispettare precisi obblighi e limiti, fra i quali si individuano:

- Risk assessment adeguato e adozione di misure di sicurezza;
- Garantire la correttezza dei data-sets e minimizzare il rischio di risultati discriminatori;
- Garantire la tracciabilità dei risultati mediante sistemi di logging;
- Set documentale che illustri chiaramente tutte le caratteristiche del sistema, nell'ottica di favorire la verifica delle autorità di controllo in ordine alla compliance del sistema;
- Informativa chiara e trasparente agli utenti;

- Misure robuste di cybersecurity.

Per i sistemi AI di riconoscimento facciale biometrico utilizzati dalle forze dell'ordine per ragioni di law enforcement, pur rientrando in questa classe, i limiti saranno molto più stringenti. Il loro utilizzo da parte della pubblica autorità sarà consentito solo in casi eccezionali, quali la ricerca di un soggetto smarrito o ai fini di prevenzione di una specifica ed imminente minaccia terroristica.

A riguardo, l'"European Data Protection Board" (cd. "EDPB", il Garante Privacy europeo) ha manifestato un po' di malumore verso la scelta della Commissione di non inibire completamente l'utilizzo di questi strumenti, ritenendoli misure di sorveglianza di massa che avrebbero meritato limiti ulteriori rispetto a quelli correlati al solo utilizzo per ragioni di law enforcement.

3. Rischio limitato

Per questi sistemi viene introdotto solo un generale obbligo di informazione trasparente e chiara a vantaggio degli utenti, i quali dovranno essere facilmente messi a conoscenza di stare interagendo con un sistema artificiale. Rientrano in questa categoria le chatbot.

Oltre a questa imposizione generale, potrebbero poi accompagnarsi obblighi più specifici. Ad esempio, in riferimento ai sistemi di "deep fake", dovrà essere specificato che il contenuto creato è artificiale e deriva da una manipolazione di altro contenuto.

4. Rischio minimo

Sarà libero e privo particolari obblighi l'utilizzo dei sistemi AI a rischio minimo, quali i sistemi di filtraggio spam o l'AI implementata nei videogames.

Ogni Stato designerà la propria Autorità di controllo mentre a livello centrale sarà creato il European Artificial Intelligence Board, autorità che dovrebbe ricalcare il modello dell'European Data Protection Board.

Lo stesso vale per il sistema sanzionatorio, che si articolerà su tre fasce:

1. per l'utilizzo dei sistemi proibiti o per la mancata implementazione dei sistemi di data governance previsti per i sistemi ad alto rischio, la sanzione potrà arrivare a 30 milioni di euro o al 6% del fatturato globale medio annuo;

2. per la violazione degli altri obblighi, l'ammontare arriva fino a 20 milioni o il 4% del fatturato globale medio annuo;
3. per la violazione degli obblighi informativi o di notificazione degli eventuali incidenti di sicurezza verso le autorità di controllo, è prevista una fascia sanzionatoria ad hoc che può arrivare a 10 milioni o al 2% del fatturato globale medio annuo.

In generale, nella proposta di Regolamento si prevedono regole di trasparenza armonizzate applicabili a tutti i sistemi di AI, e vengono individuate le seguenti pratiche vietate di Intelligenza Artificiale, in quanto contrarie ai principi dell'Unione ed ai suoi diritti fondamentali:

a) l'immissione sul mercato, la messa in servizio o l'uso di sistemi di AI che utilizzino tecniche subliminali al di là della consapevolezza di una persona al fine di falsare in misura rilevante il comportamento di una persona, in modo tale da provocare o da poter causare a tale persona o ad un'altra persona un danno fisico o psicologico;
b) l'immissione sul mercato, la messa in servizio o l'uso di sistemi di AI che sfruttino qualsiasi vulnerabilità di un gruppo specifico di persone, per la loro età o disabilità fisica o mentale, al fine di falsarne in misura rilevante il comportamento in un modo che provochi o possa provocare danni fisici o psicologici agli stessi o ad altri;
   - l'immissione sul mercato, la messa in servizio o l'uso di sistemi di AI da parte di pubbliche autorità o per loro conto, che valuti o classifichi l'affidabilità delle persone fisiche per un determinato periodo di tempo sulla base del loro comportamento sociale o caratteristiche o della personalità, note o previste, mediante un punteggio sociale che determini uno o entrambi i seguenti elementi: un trattamento pregiudizievole o sfavorevole di talune persone fisiche o di interi gruppi di persone fisiche in contesti sociali che non hanno alcun rapporto con i contesti con cui i dati sono stati originariamente generati o raccolti;
   - un trattamento pregiudizievole o sfavorevole di talune persone fisiche o di interi gruppi di persone fisiche che sia sproporzionato rispetto alla gravità del loro comportamento sociale;
c) l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico ai fini dell'applicazione della legge, a meno che e nella misura in cui tale uso sia strettamente necessario per uno dei seguenti motivi:
   - la ricerca mirata di potenziali vittime di crimini, inclusi i bambini scomparsi;

- la prevenzione di specifiche e imminenti minacce alla vita di persone o di attacchi terroristici;
- l'accertamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore del reato o sospettato di un reato punibile con una pena o una misura massima di almeno tre anni. Per l'uso di tali sistemi di identificazione biometrica vengono comunque definiti una serie di specifici requisiti.

Considerato che l'iter legislativo europeo potrebbe avere una durata massima di 18 mesi, il Regolamento definitivo potrebbe arrivare nel 2022. A ciò si aggiunga che, data la sua portata, il legislatore europeo potrebbe ragionevolmente prevedere un periodo di adeguamento a vantaggio dei consociati, durante il quale il Regolamento sarebbe sospeso nella sua efficacia. Se questo periodo fosse di 2 anni, come è stato per il GDPR, gli effetti del Regolamento potrebbero dover attendere il 2024 inoltrato prima di iniziare a dispiegarsi.

Inutile dire che per un settore come quello dell'intelligenza artificiale, il Regolamento rischierebbe quindi di nascere già obsoleto.

Ovviamente l'adozione del Regolamento si rifletterà in un aumento di costi per le imprese, che secondo uno studio realizzato per la Commissione Europea, il costo per le imprese potrebbe essere pari al 17% del valore degli investimenti totali effettuati in intelligenza artificiale.

Appare chiaro che il Regolamento riguarda la creazione di un "mercato europeo dell'AI" fin dal suo primo "Considerando". Esso, infatti, individua lo scopo del Regolamento nel migliorare il funzionamento del mercato interno definendo un quadro giuridico uniforme, in particolare per lo sviluppo, la commercializzazione e l'uso dell'intelligenza artificiale, conformemente ai valori dell'Unione.

Nel medesimo giorno di uscita della proposta di Regolamento, la Commissione ha anche proposto:

- un "*Piano coordinato di revisione dell'intelligenza artificiale 2021*", che pone le basi affinché la Commissione e gli Stati membri collaborino nell'attuazione di azioni congiunte ed eliminino la frammentazione dei programmi di finanziamento, delle iniziative e delle azioni intraprese a livello dell'UE e dei singoli Stati membri;
- il "*Regolamento del Parlamento europeo e del Consiglio relative alle macchine*", che dovrebbe sostituire la direttiva 2006/42/CE del 17 maggio 2006 relativa alle macchine, che garantisce la libera

circolazione delle macchine all'interno del mercato UE ed assicura un alto livello di protezione per gli utenti e altre persone esposte.

Tutte le soprarichiamate proposte sono il risultato di un lungo dibattito europeo sulla necessità di costruire un mercato UE dell'AI che sia affidabile, sicuro e rispettoso dei diritti fondamentali.

Il legislatore dell'UE non è quindi interessato a definire che cosa è l'Intelligenza Artificiale, preferendo invece riferirsi a quelle tecniche e approcci elencati nell'Allegato I del Regolamento che mirano, per un dato insieme di obiettivi definiti dall'uomo, a generare risultati come contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono.

Tali tecniche ed approcci elencati nell'allegato I sono relativi:

- all'apprendimento automatico, incluso l'apprendimento supervisionato, non supervisionato e di rinforzo, utilizzando un'ampia varietà di metodi incluso il cd. "deep learning";
- agli approcci logic e knowledge-based, compresa la rappresentazione della conoscenza, la programmazione induttiva (logica), le basi di conoscenza, i motori di inferenza e deduzione, il ragionamento (simbolico) e i sistemi esperti;
- approcci statistici, stima bayesiana, metodi di ricerca e ottimizzazione.

Si tratta di tecniche ben note e ampiamente utilizzate, ma l'intelligenza di questo meccanismo è la facilità con cui è possibile assoggettare al Regolamento prodotti non precedentemente inclusi aggiungendo semplicemente nuove tecniche all'Allegato I.

Per quanto riguarda l'integrazione con la legislazione già in vigore, il Regolamento considera come ad alto rischio i prodotti già soggetti a regolamentazione settoriale, garantendo in tal modo la copertura sia del mercato orizzontale che verticale delle AI (art. 6).

Per tenere conto del progresso tecnico, la Commissione inoltre ha il potere di aggiornare alcuni degli allegati del Regolamento ed in particolare:

- l'Allegato I, determinando de facto quali tecniche o approcci devono essere considerati sistemi di AI e quindi quali prodotti sono soggetti al Regolamento (art. 4);

- L‘Allegato III, determinando quali prodotti debbano essere considerati ad alto rischio per il loro impatto sui diritti fondamentali (art. 7). Questo potere incontra sostanzialmente due limiti se non teniamo conto della revoca di cui si dirà più avanti:
  - la Commissione può aggiungere prodotti ad alto rischio solo nei settori già inclusi nell‘Allegato III; i prodotti devono inoltre avere un impatto sui diritti fondamentali pari o superiore a quello dei progetti già menzionati nell‘Allegato II (*Elenco della normativa di armonizzazione dell’Unione*), tenendo conto dei seguenti criteri:
    a. lo scopo previsto del sistema di AI;
    b. in quale misura un sistema di AI è stato usato o potrebbe essere usato;
    c. in quale misura l‘uso di un sistema di intelligenza artificiale ha già causato un danno impattando negativamente sui diritti fondamentali o ha dato luogo a preoccupazioni significative in relazione al danno, come dimostrato da relazioni o accuse documentate presentate alle autorità nazionali competenti;
    d. la portata potenziale di tale danno o di tale impatto negativo, in particolare in termini di intensità e di capacità di colpire una pluralità di persone;
    e. in quale misura le persone potenzialmente danneggiate dipendono dal prodotto e se è possibile rinunciare a tale risultato;
    f. in quale misura le persone potenzialmente danneggiate si trovano in una posizione vulnerabile a causa di uno squilibrio di potere, di conoscenze, di circostanze economiche o sociali o di età;
    g. in quale misura i risultati che hanno un impatto sulla salute o sulla sicurezza delle persone sono reversibili;
    h. in quale misura la legislazione esistente dell’Unione prevede misure riparative in relazione ai rischi posti da un sistema di AI, con l’esclusione delle richieste di risarcimento, e/o misure efficaci per prevenire o ridurre sostanzialmente tali rischi.
- l‘Allegato V sulla dichiarazione di conformità UE;
- l‘Allegato VI sulla procedura di valutazione della conformità basata sul controllo interno;
- l‘Allegato VII sulla conformità basata sulla valutazione del sistema di gestione della qualità e sulla valutazione della documentazione tecnica che obbliga gli operatori economici a essere conformi ai requisiti per mitigare i rischi elevati.

In altre parole, la Commissione ha il potere sostanziale di intervenire nel mercato dell'AI al di fuori delle procedure legislative consuete, limitato solo dal potere del Parlamento europeo o del Consiglio di revocare tale potere in qualsiasi momento (art. 73).

Infine, il Regolamento incoraggia gli Stati membri a creare sistemi di sandbox regolamentati (art. 53). Le sandbox sono ambienti monitorati e controllati dalle autorità per facilitare lo sviluppo e la sperimentazione di sistemi innovativi di AI sotto una rigorosa supervisione normativa, prima che questi sistemi siano immessi sul mercato o messi in servizio in altro modo. Il meccanismo è, quindi, progettato per incoraggiare la ricerca e l'innovazione senza danneggiare gli utenti.

L'esperienza ci dice che il recupero dei dati personali senza limitazioni è stata la spinta verso importanti conquiste, tra cui il deep learning e AI, ma è anche vero che il prezzo pagato è stata la violazione della nostra privacy con risultati deplorevoli (vedi gli scandali Cambridge Analytica e TikTok).

5.3 Punti in comune con il Regolamento Generale sulla Protezione dei Dati

Considerando che i dati sono attualmente alla base dei sistemi di AI, non deve sorprendere che il Regolamento sull'AI abbia diversi punti in comune con il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati – RGPD o GDPR).

Il primo importante punto comune è che entrambi i regolamenti stabiliscono restrizioni de facto per gli operatori economici non-UE nella circolazione dei loro beni e servizi nell'UE in ragione di diritti riconosciuti come fondamentali dall'UE, da varie carte costituzionali nazionali e da trattati internazionali, come la Dichiarazione universale dei diritti umani. Inoltre, proprio perché queste restrizioni sono giustificate dalla necessità di proteggere diritti fondamentali, l'UE non sembra violare gli accordi internazionali che stabiliscono regole per la rimozione delle barriere alla libera circolazione di beni e servizi, come l'Accordo generale sul commercio dei servizi (GATS).

Un altro punto in comune è l'ambito territoriale. In entrambi i casi le regole si applicano indipendentemente dal fatto che gli operatori economici come i fornitori o i titolari o i responsabili del trattamento siano stabiliti nell'UE (v. art. 2 del Regolamento AI e l'art. 3 del RGPD).

In un sistema globalizzato di commercializzazione di beni e servizi immateriali che non ha confini e che non è necessariamente localizzato in un territorio (si pensi ai sistemi cloud), questa soluzione significa essenzialmente stabilire regole che coprono non solo l'accesso al mercato dell'UE ma anche, più diffusamente, l'accesso ai suoi consumatori e utenti.

In termini generali, le soluzioni legislative del Regolamento sono le stesse di quelle del GDPR.

Si pensi, ad esempio:

- alla valutazione del rischio di impatto sui diritti fondamentali e le soluzioni di mitigazione. A differenza del GDPR, che richiede che la valutazione del rischio di impatto sulla protezione dei dati sia effettuata dal responsabile del trattamento o dal titolare dei dati, nel Regolamento la valutazione del rischio è principalmente predisposta dal Regolamento e dalla Commissione (con riferimento all'art. 24 RGPD e all'approccio al rischio per la valutazione di impatto sui diritti fondamentali del Regolamento di cui alla tabella mostrata sopra);
- all'uso di sistemi per monitorare e certificare il rispetto delle regole (v., ad esempio, l'art. 42 RGPD e l'art. 44 del Regolamento);
- all'utilizzo delle autorità per supervisionare e controllare il mercato (v. capitolo VI del RGPD ed il Titolo VI del Regolamento);
- la previsione di multe e sanzioni in caso di infrazioni (v. capitolo VIII del RGPD ed il Titolo X del Regolamento).

5.4 Intelligenza artificiale e proprietà intellettuale

Il modo in cui si configurano i diritti di proprietà intellettuale nel contesto dell'intelligenza artificiale sta diventando particolarmente complesso alla luce dello sviluppo di algoritmi sempre più sofisticati. Come hanno dimostrato alcuni casi giurisprudenziali recenti, oggi la questione non si limita più a stabilire chi

sia proprietario di un software, ma si spinge ben oltre, fino a ipotizzare la titolarità di diritti di proprietà intellettuale in capo alle stesse IA.

Per orientarsi tra tanti dubbi ed interrogativi posti dal diritto delle nuove tecnologie e trovare soluzioni ai casi che a volte raggiungono il limite del fantascientifico, ma che si pongono con sempre maggior frequenza è necessario distinguere la proprietà intellettuale dello sviluppatore di IA, dalla proprietà del prodotto creato dall'AI (proprietà dell'AI?)

È ormai pacifico che gli algoritmi su cui si basano le IA siano dei veri e propri "metodi matematici" ai sensi della Convenzione sul brevetto europeo, che ne stabilisce la non brevettabilità (al pari delle scoperte e teorie scientifiche). L'articolo 52 della Convenzione, infatti, tutela le invenzioni "che siano nuove, implichino un'attività inventiva e siano atte ad avere un'applicazione industriale", escludendo esplicitamente i metodi matematici da tale categoria. Quando si tratta di proprietà intellettuale, è necessario infatti tenere conto di due esigenze contrapposte. Da un lato abbiamo l'importanza di remunerare il creatore dell'invenzione, in modo da incentivarne il lavoro. Dall'altro, le opere dell'ingegno sono beni immateriali e, quindi, non rivali: il loro utilizzo simultaneo da parte di più soggetti non ne diminuisce il valore, anzi, aumenta la possibilità che altri individui, a partire da quell'opera, arrivino a creare nuove invenzioni. Questa caratteristica delle opere dell'ingegno ne rende auspicabile la libera circolazione, che viene però limitata dai diritti di proprietà intellettuale. Alla base dell'esclusione dell'articolo 52 della Convenzione sul brevetto europeo c'è proprio l'esigenza di favorire lo scambio di informazioni, che in alcuni casi di "conoscenza basilare" (si pensi a un teorema scientifico!) prevalga sull'importanza di remunerare il creatore.

Tuttavia, il paragrafo 3 dell'articolo 52 contiene le premesse per la brevettabilità di algoritmi che siano utilizzati come parte di un sistema di IA che contribuisce a produrre un effetto tecnico ulteriore: se il metodo matematico è parte di un sistema più complesso, che abbia tutti gli elementi delle invenzioni stabiliti nel primo paragrafo dell'articolo 52 (novità, attività inventiva e applicazione industriale), allora l'intero sistema è brevettabile, comprensivo del metodo matematico utilizzato. Ai sensi della normativa vigente, dunque, sembrerebbe che possa essere brevettato un sistema di intelligenza artificiale nel suo complesso, se rispetta i requisiti detti sopra, ma non l'algoritmo in sé.

Vi è inoltre un ulteriore profilo di tutela del lavoro dello sviluppatore: il software è protetto dalla normativa sul diritto d'autore, per quanto riguarda gli elementi frutto ed espressione della creatività dell'autore. Siamo di fronte a un vero e proprio testo e, quindi, viene trattato dal copyright come se si trattasse di un romanzo.

Tuttavia, è già capitato che giudici ed organismi europei si siano trovati a dover decidere dei casi piuttosto bizzarri, essendo state loro sottoposte delle domande di brevetto che indicavano come autore delle invenzioni un'AI. In tale contesto, è recente la notizia del rifiuto da parte dell'EPO di riconoscere sistemi di IA quali titolari di brevetti (EP 18 275 163 ed EP 18 275 174). Nell'agosto 2019, è stato annunciato il deposito di due brevetti internazionali per "invenzioni generate dall'IA", vale a dire, invenzioni generate autonomamente da un'intelligenza artificiale, senza l'intervento di alcuna persona fisica che possa assumere la qualifica di inventore. Nel rifiutare l'istanza di deposito, l'EPO ha ovviamente sottolineato la necessità che l'inventore sia una persona fisica (v. *Responsabilità civile, etica e tutela dei diritti di proprietà intellettuale nei sistemi di intelligenza artificiale* di Vanessa Cocca - Associate CRCLEX, Milano su "Il quotidiano giuridico del 14.4.2021").

Si tratta di situazioni che andranno probabilmente ad aumentare, e non solo per richieste di brevetti: oggi esistono AI capaci di creare dipinti, come Next Rembrandt che genera nuovi quadri sullo stile del noto pittore, o altre opere d'arte come nel caso di Aiva, AI che crea nuove composizioni musicali. Ma è possibile porre in capo a una intelligenza artificiale un diritto di proprietà intellettuale?

La risposta, in realtà, è ancora più generale: a oggi, le IA non possono essere considerate titolari di diritti, perché non hanno personalità giuridica. È quello che ha affermato l'Ufficio Europeo dei Brevetti nella sua Decisione del 27 gennaio 2020, oltre che la High Court inglese nella sentenza del 21 settembre 2020.

Lo sviluppo di algoritmi di intelligenza artificiale sempre più sofisticati, in grado di svolgere molte attività come se fossero svolte dall'uomo, rischia di confondere sulla natura delle AI stesse. Il rischio è quello di umanizzare quelli che, di fatto, sono solamente degli strumenti, attribuendo agli stessi caratteristiche e diritti che sono intrinsecamente collegati con la personalità umana.

A oggi, ogni software, anche imitativo dell'intelletto umano, manca di una soggettività giuridica, pertanto, a chi dovremmo riconoscere, in ambito di proprietà intellettuale, la titolarità dei relativi diritti di utilizzazione economica o anche la responsabilità di possibili plagi o contraffazioni di opere altrui?

La proprietà intellettuale si riferisce alle creazioni della mente, come le invenzioni, opere letterarie e artistiche, disegni, e simboli, nomi e immagini utilizzati nel commercio. I diritti conferiscono, al proprietario del lavoro, diritti esclusivi di sfruttamento e beneficio dalla sua creazione.

Nella normativa italiana l'Art 2580 c.c. ("*Il diritto di autore spetta all'autore ed ai suoi aventi causa nei limiti e per gli effetti fissati dalle leggi speciali*") sembrerebbe escludere una titolarità in capo a un software, distinto dal suo creatore o proprietario.

Diversamente, Il Copyright, Designs and Patent Act (CDPA) britannico del 1988, stabilisce che è autore dell'opera prodotta tramite software (esclusi i moral rights), colui che ha effettuato le configurazioni necessarie alla sua creazione, a patto che l'opera sia "*originale*" e soddisfi il requisito di "*creazione intellettuale*" propria dell'autore, riflettendone la personalità e le scelte creative; nondimeno, sempre la legislazione del Regno Unito precisa che la riproduzione di un'opera coperta da copyright è vietata attraverso qualsiasi mezzo elettronico, ivi includendo anche gli elaborati che non rappresentano l'opera finale in sé e pertanto riprodurre, in pieno processo e sviluppo IA, un'opera coperta da copyright, comporterebbe comunque una violazione.

Il 20 ottobre 2020, il Parlamento Europeo ha adottato una Risoluzione (l A9- 0176/2020) concerne proprio la tutela dei diritti di proprietà intellettuale dell'AI nella quale, si sottolinea l'importanza della definizione di un quadro giuridico europeo adeguato per i diritti di proprietà intellettuale per l'IA e le innovazioni in materia di connettività. Nello specifico, il Parlamento ricorda che tali tecnologie si basano su modelli computazionali e algoritmi, che sono considerati metodi matematici secondo la Convenzione di Berna (CBE) e dunque non brevettabili in quanto tali. Tuttavia, ai sensi dell'articolo 52(3) della CBE, metodi matematici e programmi per computer possono essere brevettati quando sono utilizzati come parte di un sistema di IA che contribuisce alla creazione di un effetto tecnico ulteriore. Evidenzia anche il problema di richiedere una descrizione completa della tecnologia sottostante, che può essere problematica per alcune tecnologie IA data la complessità del ragionamento alla base.

Il Parlamento sottolinea poi che il coinvolgimento di sistemi di IA nel processo creativo di generazione di contenuti di carattere artistico può sollevare interrogativi riguardo alla titolarità dei diritti relativi a tali contenuti. Particolare evidenza è, a tal proposito, posta sulle differenze tra le creazioni umane ottenute con l'assistenza dell'IA e quelle generate autonomamente dall'AI. Ed è proprio in relazione a tale ultima categoria che si pongono nuove sfide normative in termini di protezione dei diritti di proprietà intellettuale, quali ad esempio le questioni della titolarità e della paternità dell'inventore.

In tale contesto, è recente la notizia del rifiuto da parte dell'EPO di riconoscere sistemi di IA quali titolari di brevetti (EP 18 275 163 ed EP 18 275 174). Nell'agosto 2019, è stato annunciato il deposito di due brevetti internazionali per "invenzioni generate dall'AI", vale a dire, invenzioni generate autonomamente da un'intelligenza artificiale, senza l'intervento di alcuna persona fisica che possa assumere la qualifica di inventore. Nel rifiutare l'istanza di deposito, l'EPO ha sottolineato la necessità che l'inventore sia una persona fisica.

Infine, il Parlamento riconosce il potenziale delle tecnologie AI nell'ambito della tutela dei diritti di proprietà intellettuale: ci si riferisce, a titolo di esempio, all'utilizzo di AI per la procedura di registrazione per la concessione dei diritti di proprietà industriale o per la determinazione della responsabilità in caso di violazione dei diritti di proprietà intellettuale. In tutte queste circostanze, il Parlamento, pur sottolineando il potenziale dell'applicazione dell'AI in suddetti ambiti, osserva non si possa sostituire l'esame umano effettuato caso per caso, al fine di garantire la qualità e l'equità delle decisioni.

Identificare un sistema di intelligenza artificiale come "inventore" richiederebbe, in buona sostanza, non solo che accettassimo il fatto che un sistema di AI possa essere equiparato alle persone fisiche, ma il pieno riconoscimento di diritti di natura legale agli algoritmi di AI.

Ad oggi, la maggior parte dei paesi, condivide la posizione dell'Ufficio Europeo dei brevetti: USA; Giappone, Cina, Corea, Germania, Francia, Inghilterra hanno espresso infatti posizioni del tutto similari per quanto concerne i diritti degli algoritmi di AI.

Sono sempre di più i sistemi di intelligenza artificiale evoluti che consentono di generare del contenuto creativo o inventivo, e noi stessi dovremo sicuramente nei prossimi anni rivedere parte delle nostre "certezze legali" per dare una risposta a queste evoluzioni tecnologiche.

Verrebbe quindi cambiata non soltanto la nostra visione, “antropocentrica”, del diritto e si arriverà forse ad introdurre, dopo la personalità fisica e quella giuridica, anche una personalità “elettronica”?

Forse siamo all'alba di un nuovo soggetto giuridico: il “robot”, cui però non sarebbe sufficiente applicare, per esteso, l’art 6 della legge sul diritto d’autore (L.633/1941) che dispone: «*Il titolo originario dell’acquisto del diritto di autore è costituito dalla creazione dell’opera, quale particolare espressione del lavoro intellettuale.*» Rimarrebbe comunque esclusa, da un eventuale riconoscimento, la possibilità dello sfruttamento economico da essa derivante!

CAPITOLO 6 - PROFILI ETICI *a cura di Federica Saraceni e Sabrina Panfili*

https://www.econopoly.ilsole24ore.com/2021/06/21/intelligenza-artificiale-regole-ue/

6.1 Le Linee Guida adottate a livello europeo[40]

Le *Linee guida etiche finali per un'intelligenza artificiale affidabile,* rese pubbliche l'8 aprile 2019, raccolgono gli orientamenti di un gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale, istituito dalla Commissione europea nel giugno 2018.

Il documento si incentra sulla necessità di promuovere un'AI affidabile, vale a dire basata su tre componenti che dovrebbero essere presenti durante l'intero ciclo di vita del sistema:

a) legalità: l'AI deve ottemperare a tutte le leggi e ai regolamenti applicabili,

b) eticità: l'AI deve assicurare l'adesione a principi e valori etici,

[40] Cfr. "Orientamenti etici per un'IA affidabile" Pubblicato il 8-11-2019 a cura della Commissione europea Direzione generale delle Reti di comunicazione, dei contenuti e delle tecnologie.

c) robustezza: dal punto di vista tecnico e sociale poiché, anche con le migliori intenzioni, i sistemi di AI possono causare danni non intenzionali.

Ciascuna componente in sé è necessaria ma non sufficiente per realizzare un'AI affidabile.

Idealmente, le tre componenti operano armonicamente e si sovrappongono; qualora, nella pratica, si dovessero verificare tensioni tra di esse la società dovrebbe adoperarsi per risolverle.

Solo con un approccio affidabile sarà possibile consentire una competitività ed una innovazione responsabile, gettando le basi affinché tutti coloro che hanno a che fare con sistemi di AI possano essere certi che la progettazione, lo sviluppo e l'utilizzo di tali sistemi sono leciti, etici e robusti.

L'etica costituisce senza dubbio un pilastro fondamentale per sviluppare un approccio all'AI volto a favorire, rendere possibile e salvaguardare la prosperità umana a livello individuale e il bene comune a livello sociale. Solo garantendo l'affidabilità i cittadini potranno trarre il massimo vantaggio dai sistemi di AI, certi del fatto che sono state adottate misure di salvaguardia contro i suoi rischi potenziali.

Molti dei rischi indicati nelle Linee Guida ricadono già nel campo di applicazione di norme giuridiche vigenti, che sono vincolanti e devono quindi essere rispettate. Tuttavia, anche quando l'osservanza delle norme giuridiche sia dimostrata, resta il fatto che tali norme potrebbero non risolvere le preoccupazioni etiche che possono insorgere. Poiché il nostro modo d'intendere l'adeguatezza delle norme e dei principi etici invariabilmente evolve e muta nel tempo, la serie non esaustiva di esempi di preoccupazioni riportata nel documento, potrà in futuro essere ridotta, ampliata, modificata o aggiornata.

Nelle Linee Guida sono riportati alcuni esempi di serie preoccupazioni destate dall'AI ed in particolare:

a. Identificazione e tracciamento degli individui con l'AI

L'IA permette a organismi pubblici e privati di identificare in modo sempre più efficiente le singole persone. Esempi degni di nota di una tecnologia scalabile di identificazione tramite AI sono il riconoscimento facciale e altri metodi di identificazione involontaria che utilizzano dati biometrici (ad esempio il rilevamento della menzogna, la valutazione della personalità in base a micro espressioni e il rilevamento automatico della voce). Identificare una persona talvolta è un atto auspicabile e rispettoso dei principi etici (ad esempio nei casi di frode, riciclaggio di denaro o finanziamento del terrorismo).

L‘identificazione automatica, tuttavia, desta enormi preoccupazioni di natura sia giuridica che etica, in quanto può avere effetti non previsti sotto molti aspetti a livello psicologico e socioculturale. Per salvaguardare l‘autonomia dei cittadini europei è necessario ricorrere alle tecniche di controllo tramite l’AI in modo proporzionato. Definire chiaramente se, quando e come l’AI può essere utilizzata per l’identificazione automatica degli individui e differenziare tra l‘identificazione di un individuo e la sua tracciatura e localizzazione, e tra sorveglianza mirata e sorveglianza di massa, sarà fondamentale per ottenere un’AI affidabile. L’applicazione di tali tecnologie deve essere chiaramente motivata dal diritto vigente. Se la base giuridica di tale attività è rappresentata dal “consenso” dell’interessato, devono essere sviluppati mezzi pratici che permettano di dare un consenso eloquente e verificato ad essere identificati automaticamente da un sistema di AI o da tecnologie equivalenti. Ciò vale anche per l‘utilizzo di dati personali “anonimizzati” che possono essere ripersonalizzati.

b. Sistemi di AI nascosti

Gli esseri umani dovrebbero sempre sapere se stanno interagendo direttamente con un altro essere umano o con una macchina e spetta agli operatori del settore dell’AI la responsabilità di comunicarlo in modo affidabile. Gli operatori del settore dell’AI dovrebbero pertanto garantire (ad esempio tramite clausole di esclusione della responsabilità chiare e trasparenti) che le persone siano consapevoli del fatto che stanno interagendo con un sistema di AI o che possano chiedere informazioni in merito e approvare tale interazione. Va notato che esistono casi limite che complicano la questione (ad esempio una voce umana filtrata da un sistema di AI). Occorre tenere presente che la confusione tra esseri umani e macchine potrebbe avere molteplici conseguenze quali attaccamento, influenza o svilimento dell’essere umano. Lo sviluppo di androidi dovrebbe pertanto essere oggetto di un’attenta valutazione etica.

c. Valutazione per punteggio dei cittadini tramite l’AI in violazione dei diritti fondamentali

Nelle società, libertà e autonomia di tutti i cittadini dovrebbero essere tutelate. Qualsiasi forma di valutazione per punteggio delle persone può comportare la perdita di tale autonomia e compromettere il principio di non discriminazione. La valutazione per punteggio dovrebbe essere utilizzata solo se esiste una chiara giustificazione e se le misure sono proporzionate ed eque. La valutazione normativa dei cittadini per punteggio (valutazione generale della “personalità morale” o dell’“integrità etica”), in tutti gli aspetti e su larga scala, effettuata da autorità pubbliche o soggetti privati compromette questi valori,

soprattutto se utilizzata in violazione dei diritti fondamentali, in modo sproporzionato e senza uno scopo legittimo descritto e comunicato all'interessato.

Al giorno d'oggi la valutazione delle persone per punteggio si utilizza spesso, su larga o piccola scala, per scopi puramente descrittivi e specifici del settore (ad esempio, nei sistemi scolastici, nell'ambito dell'e-learning e per le patenti di guida), ma anche in questi casi più limitati, dovrebbe essere disponibile una procedura pienamente trasparente, che fornisca informazioni sul processo, sullo scopo e sulla metodologia di attribuzione del punteggio. Va notato che la trasparenza non può impedire la discriminazione né garantire l'equità e non è la panacea contro il problema della valutazione per punteggio. Idealmente, quando possibile, dovrebbero essere previste modalità per dissociarsi dal meccanismo di valutazione per punteggio, senza subire alcun pregiudizio, altrimenti dovrebbero essere previsti meccanismi per contestare e rettificare il punteggio. Ciò è particolarmente importante in situazioni in cui esiste un'asimmetria di potere tra le parti. Le possibilità di dissociazione dovrebbero essere garantite nella progettazione della tecnologia laddove si debba garantire il rispetto dei diritti fondamentali e sia necessario per una società democratica.

d. Sistemi d'arma autonomi letali (LAWS)

Attualmente, un numero imprecisato di paesi e industrie si dedica alla ricerca e allo sviluppo di sistemi d'arma autonomi letali, come missili capaci di selezionare gli obiettivi o macchine ad apprendimento automatico con abilità cognitive che consentono di decidere chi, quando e dove combattere senza l'intervento umano. Questa situazione pone interrogativi etici fondamentali, per esempio la possibilità di una corsa incontrollabile agli armamenti a un livello storicamente senza precedenti e la creazione di contesti militari in cui il controllo umano è quasi del tutto assente e i rischi di malfunzionamento non sono presi in considerazione. Il Parlamento europeo ha chiesto l'elaborazione urgente di una posizione comune giuridicamente vincolante che affronti questioni etiche e giuridiche fondamentali relative al controllo e alla supervisione da parte dell'uomo, all'accountability e all'attuazione del diritto internazionale in materia di diritti umani, del diritto internazionale umanitario e delle strategie militari. Ricordando che l'Unione europea si prefigge di promuovere la pace come sancito dall'articolo 3 del trattato sull'Unione europea, sosteniamo la risoluzione del Parlamento europeo del 12 settembre 2018 e tutti gli sforzi correlati in materia di sistemi d'arma autonomi letali.

La natura dirompente di tali preoccupazioni assieme all'attuale incertezza sui relativi sviluppi, impone una valutazione costante ed una regolamentazione di questi temi, in grado di evolversi con estrema velocità.

6.2 Le risoluzioni del Parlamento Europeo

Il 20 ottobre 2020, il Parlamento Europeo ha adottato tre risoluzioni contenenti raccomandazioni per la Commissione Europea in vista della redazione e stesura dei futuri regolamenti sull'intelligenza artificiale (IA) e in particolare:

i. *Risoluzione recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale* A9-0178/2020);
ii. *Risoluzione recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate* A9 – 0186/2020);
iii. *Relazione sui diritti di proprietà intellettuale per lo sviluppo di tecnologie di intelligenza artificiale (A9- 0176/2020)*.

Il Parlamento sottolinea che, per sfruttare in modo efficiente i vantaggi e prevenire possibili usi impropri dei sistemi di IA, nonché per evitare la frammentazione normativa nell'Unione, sia essenziale disporre una legislazione uniforme, guidata da principi etici e adeguata alle esigenze future; appare dunque fondamentale la definizione di un quadro giuridico orizzontale e armonizzato, basato su principi comuni, per garantire la certezza giuridica, fissare norme uniformi in tutta l'Unione e tutelare efficacemente i valori europei e i diritti dei cittadini.

Al capitolo 5.4 abbiamo già commentato la Risoluzione in materia di proprietà intellettuale, di seguito commentiamo le altre due:

Risoluzione in materia di responsabilità civile

La proposta trova applicazione quando "un'attività, dispositivo o processo virtuale o fisico guidato da un sistema di IA abbia arrecato un danno o un pregiudizio alla vita, alla salute, all'integrità fisica di una persona fisica, al patrimonio di una persona fisica o giuridica o abbia arrecato un danno non patrimoniale rilevante risultante in una perdita economica verificabile" (art. 2 dell'Allegato alla Risoluzione – "Raccomandazioni dettagliate per l'elaborazione di un regolamento del Parlamento Europeo e del Consiglio sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale").

L’obbiettivo è quello di definire un quadro giuridico in materia di responsabilità civile che sia da un lato in grado di rispondere alle esigenze di protezione e tutela dei cittadini e dall’altro non ponga un freno agli investimenti nell'innovazione.

In tale contesto, il Parlamento sottolinea che, pur non essendo necessaria una revisione completa dei regimi di responsabilità attualmente in vigore, la complessità e la potenziale autonomia dei sistemi di AI, come pure la molteplicità degli attori coinvolti nel settore, rappresentano una sfida significativa per l'efficacia dei quadri normativi in materia di responsabilità.

È dunque necessario porre in essere adeguamenti specifici e coordinati dei regimi di responsabilità: adeguamenti che, tuttavia, non dovrebbero condurre al riconoscimento di personalità giuridica in capo allAI. Infatti, pur essendo molto difficile ricondurre specifiche azioni di un sistema di AI ad uno specifico input umano o a decisioni adottate in fase di progettazione, è tuttavia possibile definire un quadro di responsabilità che coinvolga i soggetti attivi nella progettazione e creazione dei sistemi di AI, chi ne esegue la manutenzione o chi è investito del controllo dei rischi associati.

La risoluzione ruota intorno a un doppio regime, e nello specifico:

- *Sistemi AI ad alto rischio*: “un sistema di AI autonomo che presenta un potenziale significativo di causare danni a una o più persone in un modo che è casuale e va oltre quello che ci si può ragionevolmente aspettare” (art.15). La definizione dovrebbe essere integrata da una lista limitativa sottoposta a revisione semestrale;
- *Altri sistemi AI*: tutti quei sistemi che non rientrano nella precedente definizione.

Per quanto riguarda i sistemi di AI ad alto rischio, la risoluzione prevede un regime di responsabilità oggettiva in capo all’operatore, responsabilità che non viene meno nemmeno nel caso in cui l’operatore sostenga di aver agito operando la “*dovuta diligenza o che il danno o il pregiudizio sia stato cagionato da un'attività, dispositivo o processo autonomo guidato dal loro sistema di AI*” (art.4). Unico esonero di responsabilità per l’operatore è previsto in caso di forza maggiore.

Per quel che invece riguarda gli altri sistemi di AI, l’operatore è soggetto ad un regime di responsabilità per colpa in caso di eventuali danni o pregiudizi causati da un'attività, dispositivo o processo fisico o virtuale guidato dal sistema di AI. L'operatore non è tuttavia responsabile se riesce a dimostrare che:

- il sistema si è attivato senza che l'operatore ne fosse a conoscenza e sono state adottate tutte le misure ragionevoli e necessarie per evitare tale attivazione al di fuori del controllo dell'operatore, o;

- è stata rispettata la dovuta diligenza con lo svolgimento delle seguenti operazioni: selezionando un sistema di AI idoneo al compito e alle competenze, mettendo debitamente in funzione il sistema di AI, monitorando le attività e mantenendo l'affidabilità operativa mediante la periodica installazione di tutti gli aggiornamenti disponibili.

Per l'operatore non sarà possibile sottrarsi a responsabilità sostenendo che il danno o il pregiudizio sia stato cagionato da un'attività, dispositivo o processo autonomo guidato dal suo sistema di AI. È esclusa anche in questo caso la responsabilità dell'operatore per forza maggiore.

Una seconda, importante distinzione che troviamo all'interno della risoluzione è quella tra operatore *front-end* ed operatore *back-end*, dove con il primo si intende "la persona fisica o giuridica che esercita un certo grado di controllo su un rischio connesso all'operatività e al funzionamento del sistema di AI e che beneficia del suo funzionamento", mentre con il secondo intende " la persona fisica o giuridica che, su base continuativa, definisce le caratteristiche della tecnologia, fornisce i dati e il servizio di supporto di back-end essenziale e pertanto esercita anche un elevato grado di controllo su un rischio connesso all'operatività e al funzionamento del sistema di AI".

È importante sottolineare che, i sopracitati regimi di responsabilità, si intendono applicabili sia all'operatore front-end che a quello back-end.

Quanto agli importi dei risarcimenti, per gli operatori di IA ad alto rischio la risoluzione prevede (art.5):

- un importo massimo di due milioni di euro in caso di morte o in caso di danni alla salute o all'integrità fisica di una persona interessata in conseguenza della messa in funzione di un sistema di IA ad alto rischio;
- un importo massimo di un milione di euro in caso di danni non patrimoniali rilevanti che risultino in una perdita economica verificabile o di danni al patrimonio, anche quando vari beni di proprietà di una persona siano stati danneggiati in conseguenza di un'unica messa in funzione di un unico sistema di AI ad alto rischio.

Si segnala poi la previsione dell'obbligo per tutti gli operatori di sistemi di AI ad alto rischio di stipulare un'assicurazione per responsabilità civile che copra gli importi e l'entità del risarcimento previsti dalla proposta.

Risoluzione in materia di Etica e AI

Quanto alla risoluzione in materia di etica, essa comprende raccomandazioni sui principi etici applicabili allo sviluppo, la programmazione e l'uso di AI, robotica e tecnologie correlate.

La proposta si pone come obiettivo quello di stabilire la fiducia nell'AI e di promuoverne lo sviluppo, la diffusione e l'uso nell'Unione, in particolare fornendo agli sviluppatori e agli utenti un quadro normativo appropriato che promuova la certezza del diritto assicurando al contempo il rispetto dei diritti fondamentali, la protezione dei consumatori e il rispetto dei principi etici. Il raggiungimento di suddetti obiettivi passa dalla promozione della trasparenza e un migliore scambio di informazioni tra i cittadini e le entità coinvolte nello sviluppo, impiego o utilizzo dell'AI. La proposta si sviluppa in 24 articoli divisi in principi etici, obblighi sulle tecnologie ad alto rischio e controllo da parte degli organismi europei e nazionali. Particolare attenzione è posta alle tematiche relative al controllo dell'AI ad alto rischio tramite valutazioni sulla conformità, sulla tracciabilità e sulla responsabilità degli sviluppatori; in particolare, la risoluzione auspica l'introduzione di un certificato europeo di conformità etica e l'istituzione in ogni Stato membro di un organismo pubblico indipendente per controllare l'applicazione del regolamento. Viene poi incentivata la creazione di un sistema di salvaguardie contro pregiudizi e discriminazioni legate a razza, sesso, orientamento sessuale o religione.
Infine, vengono sottolineate le esigenze legate al rispetto dei principi posti a tutela della privacy e la limitazione dell'uso di tecnologie per l'identificazione a distanza in luoghi pubblici, come il riconoscimento biometrico o facciale.

6.3 Estratto intervista a Luciano Floridi "Etica e intelligenza artificiale: il matrimonio che crea valore economico".

A conclusione di questo capitolo dedicato ai profili etici abbiamo ritenuto interessante riportare l'estratto di un intervista a Luciano Floridi, Professore Ordinario di filosofia ed etica dell'informazione all'Università di Oxford, presso l'Oxford Internet Institute, dove dirige il Digital Ethics Lab, pubblicata il 21 Agosto 2020 sul sito www.industriaitaliana., nella quale si evidenzia come il discorso riguardante l'intelligenza artificiale sia intimamente collegato a quello dell'etica e della responsabilità. E, soprattutto, di come l'etica possa produrre valore economico.

D**. Professore, partiamo dall'inizio: che cos'è l'etica?**

R. Siamo in un contesto in cui ci sono moltissime definizioni. In generale, si può dire che per Etica intendiamo tutto l'insieme degli accorgimenti necessari per fare in modo che le "cose" vadano bene.

Ma se vogliamo essere filosoficamente corretti, dobbiamo prima di tutto distinguere tra bene e male. E questo, senza soffermarci su millenni di storia del pensiero umano, ci porta direttamente alle nuove tecnologie. Perché alcune di esse possono portare a maggiore discriminazione o a minore opacità nelle decisioni. Ad esempio, se non viene concesso un mutuo in banca e la decisione è stata presa da un software, serve un umano che renda trasparente questa scelta. E un altro che la verifichi.

D. **Ora saliamo di un gradino: come si applica l'etica all'intelligenza artificiale?**

R. In questo momento, studio una branca dell'etica che dovrebbe occuparsi di alcuni problemi abbastanza semplici da definire ma molto complessi da risolvere. Il primo è l'opacità delle decisioni prese dai sistemi artificiali. Un altro è la diffusione distribuita della responsabilità: quando grandi sistemi sempre più complessi vivono anche di intelligenza artificiale, di chi è la responsabilità? Il Boeing che si è recentemente schiantato in Etiopia ha davvero avuto soltanto un problema di software? E in quel caso la colpa è dei piloti, di chi ha fatto il loro training, di chi ha autorizzato l'uso di quel software, di chi l'ha disegnato? Questi sono problemi più eclatanti. Poi ci sono quelli più silenziosi che sono due: il primo è quello della "spintarella", ovvero il fatto che un software possa tranquillamente essere programmato per consigliare sempre di andare verso una determinata direzione, andando a cozzare con la nostra autonomia. Pensiamo a chi nasce oggi e che avrà a che fare per decenni con l'intelligenza artificiale. Si tratta di soggetti che vengono spintonati gentilmente dall'intelligenza artificiale, silenziosamente ma costantemente.

Il secondo problema silenzioso è quello di chi si sta adattando a chi. A un certo punto ci troviamo a inventare delle tecnologie che fanno le cose al posto nostro, magari anche meglio e in maniera più efficiente. E lentamente siamo noi che ci adattiamo alla macchina e non viceversa. Questa è la tecnologia passata, ma se devo impiegare un piccolo software di intelligenza artificiale per fare delle operazioni e per fare in modo che tutto fili liscio e magari devo usare un linguaggio più semplice, o evitare determinate parole, allora il risultato è che la tecnologia mi ha cambiato "in peggio", mi ha reso un po' più stupido. Questo è un rischio che stiamo correndo, anche se non lo vedo come un pericolo gravissimo. Serve però mettere un punto fermo all'interazione con l'intelligenza artificiale, ed è qui che entra in gioco l'etica.

D. **A che punto è la discussione su questo tema?**

Possiamo essere ottimisti se prendiamo in considerazione spazi temporali ampi, meno se ci soffermiamo sull'immediato. Oggi la politica, i media, tutti se ne stanno occupando, e questo è entusiasmante. Però se guardiamo a quello che è stato fatto negli ultimi cinque anni, abbiamo dei risultati più frustranti: scarsi progressi, il tema dell'intelligenza artificiale è ancora affrontato per stereotipi triti e ritriti. E per allarmismi inutili o dannosi, come abbiamo avuto modo di dire in un'altra conversazione. La verità è che è giunto il momento di fare qualcosa a livello europeo, per esempio istituire un'agenzia che faccia auditing a livello serio del settore dei software così come ora viene fatto per i medicinali o per l'agroalimentare.

D. **L'etica favorisce la creazione di valore economico?**

R. Se utilizzata correttamente, sì. E almeno per due motivi. Prima di tutto permette di creare un mondo leggermente migliore, in cui il business cresce perché la gente sta meglio. Una frase che può sembrare quasi banale ma che in realtà cela il secondo motivo: l'azienda che vuole crescere rapidamente e magari farsi comprare dal grande acquirente in poco tempo è naturale che non abbia l'etica tra i propri argomenti principali. Ma l'azienda matura, grande e internazionale, che vuole stare sul mercato per i prossimi 50 anni, deve investire anche in valore sociale, in responsabilità aziendale, per migliorare l'ambiente e via dicendo.

Applicando questi concetti al digitale, vedo che ci sono le aziende "storiche" che non hanno bisogno di essere convinte che l'etica sia parte integrante del business. Poi invece ci sono le aziende più giovani che hanno invece bisogno di essere convinte. Infine, ci sono le startup, che si poggiano in maniera molto solida sull'etica e che l'hanno compresa fin da subito. Insomma, i vecchi e i giovani hanno introiettato questi temi, la generazione di mezzo decisamente no. E se vuole crescere e prosperare, deve farlo. L'etica, inoltre, rendendo trasparenti i meccanismi decisionali e i processi di funzionamento, rende l'azienda attraente per il suo ecosistema di riferimento e ne assicura la sostenibilità nel tempo.

D. Ma **non sarà anche un po' una moda, un sistema per farsi un'immagine positiva con poco sforzo? In fin dei conti un'azienda che opera conformemente alla legge e che produce ricavi è per sé stessa etica perché garantisce un beneficio alla società e a chi ci lavora …**

R. Anche questo è vero, soprattutto perché abbiamo un sistema di leggi in Europa che permette un controllo accurato di eventuali scorciatoie. Però c'è anche da aggiungere che non esiste un limite al fare

bene le cose: farle secondo le regole è il minimo, poi c'è un livello superiore che è quello etico. C'è un minimo salariale stabilito dalla legge? Certo, ma nessuno vieta di dare uno stipendio più alto del livello base. Nessuno vieta a un imprenditore di realizzare una mensa per i dipendenti. Per questo vorrei vedere questi giganti del digitale fare molto di più, mi dispiacerebbe se pensassero di limitarsi a quello che è legale perché potrebbero fare molto di più. Ad esempio, per la buona informazione e per limitare il proliferare delle fake news online. L'etica si può e si deve applicare sempre. Anche in Italia, dove il profitto viene sempre visto come qualcosa di negativo.

[…]

D. **Nei suoi scritti Lei parla di Quarta rivoluzione mondiale, riferendosi alla rivoluzione dell'Infosfera. Ma davvero stiamo vivendo una rivoluzione?**

R. Le prime tre rivoluzioni – quella di Copernico, di Darwin e di Freud – sono di spostamento. Veniamo delocalizzati dal centro dell'universo con Copernico, dal centro del mondo animale con Darwin e dal centro del mondo mentale con Freud. Con l'Infosfera veniamo delocalizzati dal mondo dell'informazione o infosfera.

D. **Ma che cos'è esattamente l'Infosfera?**

R. È lo spazio delle informazioni in cui passiamo sempre più tempo. Prima veniva definito cyberspazio, oggi invece trovo che Infosfera sia più efficace per due motivi. Prima di tutto perché è sia analogica sia digitale e queste due dimensioni si mescolano senza soluzione di continuità. Inoltre, ci aiuta a superare l'idea che il cyberspazio aveva introdotto che per essere online era necessario connettersi. Oggi siamo sempre connessi. Per questo, insieme a Infosfera ho sviluppato il concetto di Onlife, cioè che un individuo che passeggia per strada convinto di non essere connesso, ha nel suo smartphone almeno una ventina di app che lo stanno geolocalizzando costantemente. L'Infosfera è uno spazio nuovo che stiamo costruendo e in cui passiamo sempre più tempo.

La politica sta avvenendo qui, così come le relazioni sociali, economiche e via dicendo. Tanto più l'Infosfera si allarga, tanto più diventiamo soggetti marginali perché gli agenti più funzionanti all'interno della struttura sono quelli digitali. Bisogna iniziare a immaginare gli individui come dei nodi, parte di una rete che a sua volta è immersa nell'Infosfera. Solo così si possono comprendere alcuni temi: il

successo dei social network anche in politica, la capacità di fare business anche come piccola azienda connessa e così via.

A un livello minimo, l'Infosfera indica l'intero ambiente informazionale costituito da tutti gli enti informazionali, le loro proprietà, interazioni, processi e reciproche relazioni. È un ambiente paragonabile al cyberspazio, ma al tempo stesso differente dal cyberspazio, che è soltanto una sua regione, dal momento che l'Infosfera include anche gli spazi d'informazione offline e analogici. A un livello massimo, l'Infosfera è un concetto che può essere utilizzato anche come sinonimo di realtà, laddove interpretiamo quest'ultima in termini informazionali. In tal caso, l'idea è che ciò che è reale è informazionale e ciò che è informazionale è reale.

D. **E perché si tratta di una delocalizzazione di noi stessi?**

R. Io già da qualche anno sto cercando di spiegare che le tecnologie digitali non sono soltanto straordinarie per quello che ci permettono di fare, ma anche per quello che ci permettono di capire nei confronti di noi stessi, di chi siamo, di chi vogliamo essere, di che società vogliamo costruire, delle ambizioni che possiamo soddisfare. Ho cercato di far capire che era una rivoluzione di autocomprensione, ho cominciato a guardare ad essa come se fosse una delocalizzazione di noi stessi: non siamo più neanche al centro dell'informazione, perché ci sono tanti altri oggetti che la trattano a volte anche più velocemente e in maniera più efficace.

D. **Lei dice anche che le ICT stanno rendendo l'informazione sempre più responsabile …**

R. Quanto più ciascuna informazione è distante appena un click, tanto meno saremo scusati dal non averla ricercata. Le tecnologie dell'informazione e della comunicazione stanno rendendo l'umanità sempre più responsabile, dal punto di vista morale, per il modo in cui il mondo è, sarà e dovrebbe essere. Ciò è in qualche misura paradossale, poiché le ICT sono anche parte di un fenomeno più ampio, per cui la chiara attribuzione di responsabilità a uno specifico agente individuale è diventata più difficile e controversa.

CAPITOLO 7 - RIFLESSIONI CONCLUSIVE

L'AI è indubbiamente una tecnologia trasformativa e dirompente, la cui evoluzione negli ultimi anni è stata agevolata dalla disponibilità di enormi quantità di dati digitali, oltre che dai grandi progressi tecnologici, nella potenza di calcolo, nelle capacità predittive, nell'elaborazione di metodi e strumenti sempre più innovativi.

I sistemi di AI continueranno ad avere effetti sulla società e sui cittadini che non possiamo ancora immaginare. In tale contesto, è importante realizzare sistemi di AI che siano degni di fiducia, poiché gli esseri umani potranno sfruttarne pienamente e con sicurezza i vantaggi solo se la tecnologia, i processi e le persone a monte si riveleranno affidabili.

Nei prossimi anni la domanda non sarà più se adottare l'intelligenza artificiale ma come farlo nel miglior modo possibile. I valori e i benefici dell'intelligenza artificiale possono essere eccezionali, ma deve essere chiaro che il ruolo dell'AI è quello di sostenere l'uomo e le sue attività e non quello di sostituirlo in toto. Nella partita tra l'uomo e l'AI, il diritto gioca un ruolo fondamentale e perché questo ruolo sia efficace dovrà porsi come unico obiettivo quello di mettere sempre al centro la tutela dell'uomo ed i suoi diritti: sia quando è l'uomo ad inventare ed innovare, sia quando è l'uomo ad utilizza il risultato delle invenzioni e delle innovazioni di altri uomini.

Per evitare che l'uomo venga travolto dalle sue stesse invenzioni, a fare la differenza sarà la disciplina che i vari ordinamenti adotteranno. E anche laddove si dovesse arrivare a configurare una "personalità digitale" dell'AI, il suo legale rappresentante non potrà che essere quella persona fisica in grado di averne il totale controllo!

https://www.axepta.it/intelligenza-artificiale-aziende/