IL DIRITTO APPLICATO ALLA PRODUZIONE ED ALL'IMPIEGO DI SISTEMI DI INTELLIGENZA ARTIFICIALE

N.B.: PER UNA PREPARAZIONE COMPLETA OCCORRE AFFIANCARE LE PRESENTI DISPENSE AL CONTENUTO DELLE SLIDE DISCUSSE NEL CORSO DELLE LEZIONI

I. Perché serve un "diritto per l'Intelligenza Artificiale"?

La rapida evoluzione nel settore dell'A.I. e del *machine learning*, il cui sviluppo ha conosciuto negli ultimi anni un'accelerazione senza precedenti, incidono su ogni aspetto della nostra vita (lavoro, impresa, salute, economia, giustizia, polizia, attività della pubblica amministrazione, settore bancario, socialità, mobilità, creatività, finanza, ecc.), ponendoci davanti a nuovi scenari e domande inedite, anche dal punto di vista del diritto.

Gli interrogativi più rilevanti, a livello giuridico, sorgono in relazione alla capacità della macchina "intelligente" di essere ***self-learning***, ossia di **evolvere e crescere con l'esperienza** e di **cambiare i propri meccanismi di funzionamento** (cosa, questa, ben diversa dal semplice aumento di capacità computazionale). La capacità di essere *self-learning* - che consente alla macchina di acquisire la **capacità di agire in autonomia** - pone importanti questioni con riferimento:

- sia al problema della ***explainability***, ossia la possibilità di spiegare il "perché" del comportamento dei sistemi di A.I. più avanzati;
- sia alla rilevanza della fase del ***training*** della macchina e della **qualità dei dati** alla stessa forniti.

L'ampia diffusione dell'utilizzo di forme di A.I. in diversi campi pone, altresì, interrogativi di non poco conto anche dal punto di vista etico: ci si chiede, in particolare, se si possa pretendere dalla macchina un comportamento etico e quali siano gli strumenti, anche sul piano regolatorio, per la creazione di un'**etica dell'A.I.**

Diversi sono gli interventi normativi volti a regolare il fenomeno "*Artificial Intelligence*". A livello europeo, tra i più recenti, si ricordano:

- le Linee Guida per una A.I. etica del 2019;
- la Proposta di Regolamento per un *Artificial Intelligence Act* dell'aprile 2021;
- la Proposta di Direttiva per una nuova responsabilità da prodotto del settembre 2022;
- la Proposta di Direttiva sulla responsabilità civile da A.I. del settembre 2022.

Analogamente, si registrano in Cina nuove linee guida etiche per l'A.I. e negli Stati Uniti: decine di proposte normative in materia di A.I., alcune già legge.

Anche alla luce di tali preliminari considerazioni, si delineano, dunque, i seguenti temi d'indagine:

- in che modo è consentito "produrre" un sistema di A.I.? E quali caratteristiche deve, o dovrà, avere perché sia lecito produrlo, commercializzarlo e usarlo?
- quali sono le responsabilità connesse alla produzione ed all'impiego di sistemi di A.I.? Come i soggetti coinvolti nella "filiera" della A.I. possono essere chiamati a

rispondere delle "azioni" di un sistema che non riescono a pienamente prevedere *ex ante* e comprendere *ex post*?

- quali cautele sono richieste per l'utilizzo di questi sistemi? Quale l'affidamento nelle decisioni automatizzate e quali i controlli richiesti da parte dello *human in command*?

II. La regolazione della "produzione" di Intelligenza Artificiale

II.A) Le decisioni automatizzate: trasparenza e rischi di discriminazione

I nuovi sistemi di A.I. operano sulla base di modelli non più fondati solo su un paradigma logico-deduttivo e deterministico (secondo il quale, dunque, fornendo ai "sistemi intelligenti" i medesimi *input*, ci si potrà attendere gli stessi *output*), bensì su modelli predittivi basati su correlazioni statistiche.

Le criticità - cui già si è fatto cenno - connesse a tale *modus operandi* riguardano:

- la **spiegabilità** e la **trasparenza dell'A.I.**: i sistemi operano sulla base di logiche diverse da quelle umane, con la conseguenza che i risultati ottenuti risulteranno difficilmente prevedibili *ex ante* e comprensibili *ex post*;
- il rischio di **risultati discriminatori** e ***bias* cognitivi**, sia a livello di modello di dati, sia a livello di modello di calcolo dell'A.I. (al riguardo si evidenzia la rilevanza della fase del *training* della macchina e della qualità del *data set* alla stessa fornito).

→ **Che cosa di intende per spiegabilità**? La spiegabilità è la proprietà di un sistema di poter dare una spiegazione ad un essere umano in modo soddisfacente e di poter, dunque, rispondere alla domanda "perché?".

→ **Che cosa di intende per interpretabilità**? Al fine di rispondere a questa domanda è opportuno introdurre una ulteriore fondamentale distinzione tra:

- **A.I. simbolica**, basata su regole logiche-deduttive e deterministiche (in tale categorizzazione rientrano, ad esempio, i sistemi esperti in ambito medico o giuridico);
- **AI sub-simbolica**, basata su teorie statistiche e probabilistiche (si pensi, ad esempio, i sistemi di *machine learning*, *deep neural network*, ecc.).

La prima è per definizione comprensibile e spiegabile "in modo nativo", ossia produce in modo autonomo elementi per capire il come ed il perché di un determinato *output* (si parla in questo senso di "**white box"**). La seconda, per la complessità dei parametri usati e per la natura non deterministica dei modelli adottati, non garantisce di fornire una comprensibilità diretta del meccanismo che ha prodotto un determinato esito (si parla in questo senso di "**black box"**).

→ **Come posso "aprire" il black box?**

Un primo tentativo volto a risolvere il problema della opacità dell'algoritmo e dei processi decisionali "animati" dall'algoritmo si rinviene nell'**art. 22 del GDPR** (vd. dispense su protezione dati personali), il quale disciplina le ipotesi di **trattamento dei dati interamente automatizzato**.

- Per rispondere alla domanda se le tutele ivi previste per l'interessato possano ritenersi sufficienti e quale sia il tipo di informazioni che devono essere fornite allo stesso, si rinvia, per completezza, a quanto più ampiamente esposto alle pagg.

11-13 delle dispense su "*Dati, privacy e data protection*".

- Per esempi concreti di casi in cui sono state affrontate le criticità connesse alla opacità dei sistemi di A.I., si rinvia a quanto illustrato sui "*Casi trasferimenti insegnanti*" del 2019 nelle *slide* "*La regolazione dell'Intelligenza Artificiale*".

II.B) Nuovi obblighi? Ed in capo a chi?

I soggetti coinvolti nella "filiera" in materia di A.I., sui quali possono e potrann gravare specifici obblighi ed ai quali possono essere attribuibili, a diverso titolo come si dirà *infra*, le responsabilità relative al comportamento della A.I., sono i seguenti:

- il creatore dell'algoritmo;
- il creatore/costitutore della banca dati o comunque del dataset fornito all'A.I.;
- il *trainer* dell'A.I.;
- il creatore del *software* che incorpora l'algoritmo;
- il produttore dell'*hardware* che incorpora il *software* che incorpora l'algoritmo;
- il distributore del sistema di A.I.;
- l'utilizzatore del sistema di A.I.

II.C) La regolazione dell'A.I.: v. slides su Regolamento UE *Artificial Intelligence Act*

III. La responsabilità da produzione ed utilizzo dell'Intelligenza Artificiale: chi risponde dei danni causati dall'A.I.?

Come già rilevato, l'A.I. permette ai sistemi ed alle macchine autonomi ed "intelligenti" di sviluppare "*determinate caratteristiche autonome e cognitive*" e "*capacità di apprendere dall'esperienza e di prendere decisioni quasi indipendenti*" (Risoluzione Parlamento Europeo, febbraio 2017); ed, ancora, "*l'integrazione dell'IA nei prodotti può modificare il funzionamento di tali prodotti durante il loro ciclo di vita*", perché "*gli algoritmi possono continuare a imparare mentre vengono utilizzat*i" (Libro Bianco sull'A.I. UE, febbraio 2020).

Sotto il profilo giuridico della attribuzione delle responsabilità, tali caratteristiche pongono rilevanti quesiti; ed in particolare:

- se chi progetta, programma e "produce" il sistema può non essere sempre in grado di prevedere e prevenire le reazioni che il sistema sviluppa in relazione a quanto lo circonda, come può essere responsabile degli eventuali danni dallo stesso cagionati?
- in che modo tale soggetto può essere chiamato a rispondere di qualcosa che non è in grado di prevedere ed in relazione al quale (forse) non ha colpa? Esiste il rischio di un "vuoto di responsabilità"?
- è possibile affermare che più una macchina è autonoma, meno l'essere umano deve rispondere delle sue "azioni"?

→ Ma **a chi è possibile attribuire la responsabilità** per danni causati dal sistema "intelligente", tra i soggetti coinvolti nella "filiera" della A.I (creatore/produttore, creatore dell'algoritmo, addestratore, utilizzatore…)?

→ Ed ancora: è **sufficiente il rispetto dei requisiti tecnici di produzione dell'A.I**. che dovessero essere previsti dalla legge per andare esenti da responsabilità?

III.A) La responsabilità del produttore della A.I.: la responsabilità da prodotto difettoso

Con riferimento alle responsabilità attribuibili al produttore della A.I., viene in primo luogo in rilievo la normativa - concepita a livello unionale nella Direttiva 85/374/CEE e successivamente recepita a livello nazionale nel nostro Codice del consumo - in materia di **responsabilità da prodotto difettoso (*product liability*)**.

L'**onere probatorio** gravante sul danneggiato sulla base della normativa in esame prevede che lo stesso, al fine di ottenere il risarcimento del danno subito, possa limitarsi a dare prova dei seguenti elementi:

- della **difettosità del prodotto,** laddove il "difetto" consiste in un disallineamento del prodotto rispetto agli standard che la platea di utenti ha ragionevolmente diritto di attendersi;
- del **danno patito**;
- del **nesso di causalità** tra il suddetto difetto ed il danno.

N.B. **Non** sarà, invece, necessario per il danneggiato fornire la prova della **colpa** del produttore.

Evidente è, dunque, il favore accordato al consumatore dalla disciplina della *product liability* (si segnala, tuttavia, come in ipotesi di applicazione di tale disciplina ai sistemi autonomi, tale atteggiamento di favore nei confronti del consumatore potrebbe risultare frustrato dalla caratteristica della **opacità** - talvolta anche per il produttore - **del funzionamento del sistema "intelligente**": in altri termini, potrebbe risultare arduo fornire la prova sia del difetto che della correlazione causale tra difetto e danno).

La normativa in esame - applicabile anche al produttore di una componente del prodotto, il quale può rispondere direttamente nei confronti del consumatore - prevede, altresì, un'ipotesi di **esclusione della responsabilità** per danni causati da un difetto che non poteva essere previsto in base alle conoscenze scientifiche e tecniche disponibili al momento della messa a punto del prodotto (si parla, in questo senso, del cd. "**rischio da sviluppo**").

→ È **possibile applicare la disciplina della responsabilità da prodotto difettoso all'A.I**.?

Tale domanda assume particolare rilievo per il caso dell'**Internet of Things** (IoT), caratterizzato dalla connessione tra prodotti che interagiscono in *network*, coordinando le rispettive azioni per l'attuazione di obiettivi complessi. Tale caratteristica rende particolarmente arduo il riparto delle responsabilità per eventuali malfunzionamenti del sistema, specie quando a cagionare l'evento dannoso non sia un difetto del prodotto in sé considerato, ma un difetto dell'interazione dei *device.*

→ Ma, prima ancora, l'**A.I.** può definirsi "**prodotto**" ("*standalone*")? O è una **componente** di un prodotto ("*embedded*")?

Secondo la disciplina della responsabilità da prodotto, può definirsi tale "*ogni bene mobile, anche se incorporato in altro bene mobile o immobile*" (ivi inclusa l'elettricità) e la Proposta di UE di Regolamento definisce espressamente l'A.I. come "prodotto".

→ Quando l'**A.I.** può definirsi **difettosa**? Cosa è "difetto" quando parliamo di A.I.?

Al pari di quanto previsto per gli altri beni al consumo, il difetto del prodotto *A.I.-powered* consiste nel disallineamento dello stesso rispetto agli standard ragionevolmente attesi dall'utente.

Due le categorie di difetti che possono caratterizzare un la categoria di prodotti in esame:

- difetti genetici (si pensi, ad esempio, all'inserimento nel sistema A.I. di una linea di codice errata, ad una eccessiva permeabilità dell'A.I. alle aggressioni di *hacker*);
- difetti non genetici, ossia generati nel corso del processo di apprendimento ed evoluzione.

III.B) La Proposta di Direttiva per una nuova responsabilità da prodotto (settembre 2022)

Le considerazioni sinora svolte sono state in parte recepite e taluni degli interrogativi posti hanno trovato risposta nella recente **Proposta di Direttiva sulla responsabilità da prodotto difettoso**, con la quale la Commissione europea mira a sostituire le norme attualmente vigenti - alle quali si è sinora fatto cenno - per adattarle ai nuovi prodotti a elevato contenuto tecnologico, non solo all'A.I. (provvedimento "gemello" a quello in esame è la Proposta di Direttiva sulla responsabilità civile da A.I., presentata anch'essa nel settembre 2022 e volta ad adeguare le norme esistenti in materia di responsabilità civile all'A.I.).

Tale documento - che, **allo stato**, rimane ancora una **proposta** - propone, infatti, una "*revisione alla luce degli sviluppi connessi alle nuove tecnologie, ivi inclusa l'A.I., ai nuovi modelli di business dell'economia circolare […], nonché alla luce delle criticità emerse in relazione al riparto degli oneri probatori tra consumatore e impresa, specialmente in considerazione dell'incremento della complessità scientifica*".

- ❖ Per le "nuove" definizioni di "prodotto", di "componente", di "difetto" e di "rischio da sviluppo", si rinvia alle *slide* "*Responsabilità da Intelligenza Artificiale*".

III.C) La responsabilità da attività pericolosa

Accanto alla normativa della *product liability*, in relazione ai nuovi sistemi intelligenti, viene, altresì, in rilievo quella relativa all'esercizio di attività pericolosa, disciplinata dall'art. 2050 del codice civile, il quale prevede che "*chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno*".

→ L'**A.I. è "pericolosa"** per natura? Il ricorso alla A.I. si rivela, per sua natura, suscettibile di rendere pericolose attività che altrimenti non sarebbero tali?

In questo senso parrebbe deporre anche la Proposta di Regolamento sull'A.I. che - come già accennato - espressamente individua, a monte, delle specifiche forme di A.I. che definisce **"ad alto rischio"** (tra le quali inserisce, peraltro, il settore dei trasporti, con i veicoli a guida autonoma).

Sulla base della disciplina in esame, la responsabilità dell'esercente attività pericolosa può essere esclusa solo ove lo stesso dimostri di avere adottano preventivamente **tutte** le **misure (preventive) idonee** ad evitare il danno.

→ **Quali sono le "misure idonee**"?

La valutazione dell'idoneità di tali misure dovrà esser effettuata con un **giudizio *ex ante*** in relazione all'esigenza di evitare la generale situazione di pericolosità (e non lo specifico evento lesivo) e dovrà necessariamente essere condotta alla luce delle **conoscenze e delle tecnologie esistenti al momento della produzione**.

→ **Cosa è da considerarsi "pericoloso"**? Solo la produzione, o anche la vendita, l'utilizzo…dell'A.I.?