

SCHEDA 21 Aprile 2023

# LA SFIDA DELL'INTELLIGENZA ARTIFICIALE AL DIRITTO PENALE

Cristiano Cupelli

*\*Il testo riproduce, con alcuni aggiornamenti, un articolo dell'Autore pubblicato sul quotidiano Il Foglio sabato 8 aprile 2023.*

1. Come dimostra il dibattito su potenzialità, limiti e rischi di *ChatGPT*, l'intelligenza artificiale, permeando settori sempre più estesi della quotidianità, determina l'insorgere di delicate questioni giuridiche, che hanno iniziato a interessare anche il diritto penale, storicamente più refrattario alle innovazioni tecnologiche. E che quello tra *IA* e scienza penalistica sia un rapporto destinato a un vorticoso sviluppo, non foss'altro che **per colmare il ritardo accumulato** tanto sul piano della riflessione teorica quanto su quello legislativo, è confermato dal fermento normativo, attestato da due recenti provvedimenti di matrice sovranazionale: la Risoluzione del Parlamento europeo del 6 ottobre 2021, intitolata "*L'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale*", che, pure non avendo forza vincolante, rappresenta un significativo punto di partenza per cogliere l'orientamento dell'Unione europea in rapporto ai profili di responsabilità penale collegati all'*IA* e la proposta di Regolamento europeo (c.d. *IA Act*), che stabilisce regole armonizzate

sull'intelligenza artificiale e modifica alcuni atti legislativi dell'Unione, focalizzando l'attenzione su sistemi di IA "ad alto rischio" e sull'individuazione degli obblighi e delle responsabilità che dovrebbero essere poste in capo ai fornitori dei sistemi stessi.

**2.** Approcciandosi al tema, occorre anzitutto individuare gli **ambiti** all'interno dei quali la rivoluzione tecnologica messa in moto dall'IA può significativamente impattare sulle pretese di tutela dei beni giuridici affidate al diritto penale.

Schematizzando al massimo, si possono individuare **quattro macroaree**: **a)** le attività di *law enforcement* e di giustizia predittiva (si pensi alle macchine utilizzate dalle forze di polizia, per lo più in via sperimentale, per compiti come pattugliamento, sorveglianza, disinnescamento di bombe, riconoscimento facciale, ecc.); **b)** il possibile impiego di algoritmi decisionali, dopo una sperimentazione per la decisione di liti civili o di contenziosi amministrativi, anche in ambito penale; **c)** l'uso di c.d. algoritmi predittivi (*risk assessment tools*) per la valutazione, in senso ampio, della pericolosità criminale ai fini dell'applicazione di una misura di sicurezza, di una misura cautelare o di una misura di prevenzione o anche per concedere la sospensione condizionale di una pena o l'affidamento in prova al servizio sociale; **d)** il coinvolgimento di un sistema di IA come strumento, autore o vittima di un reato.

**3.** Uno dei punti **più controversi** della riflessione investe proprio quest'ultimo profilo, e cioè il possibile coinvolgimento di un sistema di IA quale **autore di un reato**.

Gli **esempi** non mancano e sono tutti abbastanza noti: dai droni capaci di uccidere per le strade urbane (come avvenuto nella città di Dallas nel luglio 2016), alle auto senza conducente coinvolte nella causazione di incidenti a danno di cose o persone (è quanto accaduto nel marzo 2018 in Arizona) o ancora ai *software* che eseguono, in collaborazione o addirittura in sostituzione dell'uomo, compiti sempre più sofisticati (pilotare un grosso aereo) e che talvolta possono interferire negativamente con la condotta umana, come i recenti disastri aerei dei Boeing 737 Max hanno purtroppo dimostrato.

La casistica stimola un **interrogativo**, che a sua volta chiama in causa questioni più generali: in episodi simili, qualora si riscontri un fatto di reato, al di fuori dei casi in cui a rispondere sia chiamato il programmatore, il produttore o l'utilizzatore del software (allorquando, cioè, il sistema non rappresenti altro che uno strumento in mano all'uomo attraverso il quale, in ragione delle enorme potenzialità asservibili a scopi criminali, il reato possa essere realizzato), **può davvero un sistema di ultima generazione assumere le vesti di soggetto attivo del reato?**

4. Seppure non manca chi, facendo leva sul fatto che i sistemi di IA, perlomeno quelli più evoluti e sofisticati, sono capaci di agire in autonomia, di assumere ed eventualmente attuare decisioni proprie, che non erano prevedibili dai loro programmatori, offre una risposta **affermativa** (ipotizzando, in un parallelismo con la disciplina della responsabilità degli enti, una *colpa di programmazione*), le principali **perplexità**, allo stato, ruotano sulla difficoltà di ravvisare, in capo a una macchina, il tradizionale requisito della **colpevolezza**. Si tratta, come si sa, dell'espressione più intensa del coinvolgimento soggettivo dell'autore nel fatto, la cui presenza comporta la possibilità di muovere un rimprovero e che presuppone la ravvisabilità, in capo al soggetto, di imputabilità, dolo o colpa, conoscenza (o per lo meno conoscibilità) della legge penale violata e assenza di cause di esclusione della colpevolezza.

Ebbene, ci si chiede: questi elementi, originariamente concepiti e tradizionalmente riferiti solo all'umano, possono ascrivere a una macchina? è ipotizzabile una **colpevolezza robotica**, in assenza, fra l'altro, di requisiti *certi* quali l'autocoscienza, il libero arbitrio, l'autonomia morale? Si può parlare di "capacità di intendere e di volere" in relazione a un software o configurare in capo ad esso una colpa o addirittura un dolo? Ancora: quali **sanzioni** potranno essere comminate a tali sistemi e soprattutto, nel caso, saranno in grado di assolvere quelle funzioni, orientative e rieducative, che la Costituzione riconosce alla pena? E poi, all'esito di quale tipo di **processo** e con quali **garanzie**?

5. Quando gli interrogativi superano le certezze, l'unica certezza è che occorre muoversi con **cautela**. Il che, tuttavia, non giustifica la sottovalutazione del tema: se il diritto penale vuole continuare ad assolvere il proprio ruolo, deve mettersi nelle condizioni di affrontare consapevolmente le sfide, complesse ma ineludibili, dello sviluppo tecnologico, ripensando schemi classici e proponendo, senza stravolgere principi consolidati di garanzia, modelli nuovi di incriminazione e paradigmi di tutela aperti alle spinte di un futuro che bussava alla porta.