Intelligenza artificiale e diritto penale: nuove indicazioni dal Parlamento Europeo

di *Alice Giannini*

Il 6 ottobre 2021 il Parlamento Europeo ha approvato la risoluzione dal titolo "L'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale".[1] Si tratta di un documento interessante per approfondire il tema dell'impatto dell'intelligenza artificiale (IA) sulla materia penale. In particolare, in questa risoluzione è possibile intravedere le basi di quello che sarà l'orientamento europeo in due campi: da un lato quello diritto penale sostanziale, ossia le c.d. *aree di conflitto* fra l'IA e il diritto penale,[2] dove i costrutti classici del diritto penale classici faticano nello stabilire chi è responsabile; dall'altro quello della procedura penale e dell'*enforcement*, le c.d. *aree di collaborazione*,[3] dove l'IA si pone quale mezzo di miglioramento delle prassi attuali. Questo breve commento si articolerà dunque su questi due binari paralleli.

1. Aree di conflitto

Se dal lato della responsabilità civile il legislatore europeo può appoggiarsi già su solide basi, lo stesso non si può dire per quanto attiene la responsabilità penale. Una futura regolamentazione a livello europeo in questo settore, infatti, dovrebbe senza dubbio inserirsi in un dedalo di normative già esistenti – tra tutte quella relativa al danno da prodotto – nonché confrontarsi con la più debole competenza dell'Unione Europea sulla materia penale. Non esiste ad oggi un diritto penale di *parte generale* dell'Unione Europea: questo aspetto è di particolare rilevanza perché l'agire stesso dei sistemi di IA pone alle categorie dogmatiche classiche del diritto penale problematiche che sono trasversali a come i singoli codici penali dei paesi membri disciplinano gli elementi del reato. Pensiamo, dal punto di vista dell'elemento oggettivo del reato, alle difficoltà di ricostruire il nesso causale, alla luce sia della commistione dell'agire umano e dell'agire algoritmico, che dell'imprevedibilità e dell'autonomia di quest'ultimo. Dal punto di vista dell'elemento soggettivo forse le problematiche più evidenti sono quelle poste per quanto attiene all'istituto della colpa e i

[1] Parlamento Europeo, L'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale, 2020/2016(INI), 26 ottobre 2021.
[2] I. Vuletić, T. Petrašević, *Is It Time to Consider EU Criminal Law Rules on Robotics?*, 2020, 16 CYELP, p. 228.
[3] *Ibid.*

soggetti umani coinvolti nella catena di progettazione e realizzazione del sistema di IA. Si tratta dunque di capire come modellare tale istituto senza incorrere in fattispecie a responsabilità oggettiva

Ciò posto, in questa risoluzione vi è innanzitutto *una presa di coscienza esplicita* dei problemi collegati alla corretta individuazione delle responsabilità giuridica e dell'imputabilità in relazione ai potenziali effetti nocivi dei sistemi di IA utilizzati in ambito penale (art. 13). Tale constatazione, estensibile anche agli altri settori in cui l'utilizzo di tali tecnologie è in crescita (ad esempio il settore dei trasporti o quello della sanità), è legata alla complessità dello sviluppo e del funzionamento dei sistemi di IA. Infatti, come si legge nel *considerando I*, questi richiedono "il contributo di molteplici persone, organizzazioni, componenti meccanici, algoritmi software e utenti umani in ambienti spesso complessi e problematici".

Da ciò deriva l'importanza e la necessità di stabilire un modello *chiaro* ed *equo* per attribuire la responsabilità per l'utilizzo di tali sistemi nel campo della giustizia penale (art.13). Viene poi sancito che la responsabilità deve ad ogni modo ricadere *sempre* su una persona fisica o giuridica, che deve obbligatoriamente essere identificata per tutte le decisioni assunte con il supporto di un sistema di IA. In tal modo, si nega la possibilità di attribuire una qualsivoglia personalità "elettronica" all'IA, nonché di poterla ritenere direttamente responsabile. Non è chiaro però come questo modello dovrebbe essere costruito né come questa persona responsabile vada identificata.

Nella risoluzione viene poi ribadito che il primo e principale scopo di queste future norme di diritto penale debba essere la *prevenzione* di effetti negativi, ispirata al principio di *precauzione*. All'istante l'invocazione di questo principio ci riporta alle riflessioni collegate al c.d. diritto penale del rischio, riflessioni che purtroppo non è possibile affrontare in questa sede ma che sono di massimo rilievo anche alla luce dell'impostazione prescelta dall'AI Act[4] che, come si sa, è basata su un *risk-based approach*.

2. Aree di collaborazione

[4] Commissione Europea, Proposta di regolamento del parlamento europeo e del consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione, 2021/0106(COD), 21 aprile 2021.

Questa area rappresenta il *lion's share* della comunicazione qui analizzata. Il Parlamento Europeo, infatti, identifica una serie di aspetti problematici relativi all'utilizzo di sistemi di IA nella *criminal justice* che dovranno essere attenzionati dagli stati membri. Ci concentreremo qui sugli articoli più significativi.

Innanzitutto, all'articolo 14 viene ribadita l'importanza di prevedere vie di ricorso effettive contro l'utilizzo di strumenti di IA nei settori dell'attività di contrasto alla criminalità nonché nel settore giudiziario. Le parti di un procedimento penale devono avere il diritto di accedere al processo di raccolta dei dati ed agli output prodotti dallo strumento. Inoltre, secondo il Parlamento Europeo l'utilizzo di questi sistemi potrà avere un impatto anche nelle valutazioni delle autorità nazionali relative alle richieste di estradizione o consegna nei confronti di un altro paese (sia questo UE o extra-UE): in particolare queste dovranno valutare se l'utilizzo di tali strumenti possa indebolire "manifestamente" il diritto fondamentale all'equo processo sancito dall'art. 47 della Carta Fondamentale nonché dall'articolo 6 della CEDU. Tali valutazioni dovranno essere svolte seguendo una serie di orientamenti scritti che dovranno essere redatti dalla Commissione.

L'articolo 15 redarguisce gli operatori del settore contro il riporre "eccessiva fiducia nella natura apparentemente oggettiva e scientifica degli strumenti di IA" nonché nei risultati da questi prodotti. Invita inoltre le autorità ad acquisire conoscenze e dimestichezze per "*mettere in dubbio o respingere una raccomandazione algoritmica*". L'utilizzo del termine raccomandazione non è casuale: all'articolo 16, infatti, viene sancito che la decisione che produce effetti giuridici o analoghi debba essere presa sempre da un essere *umano* che possa essere ritenuto *responsabile per le decisioni adottate*. Questo articolo è uno dei più ricchi di contenuti della risoluzione: in esso, infatti, il Parlamento invita le autorità che utilizzano sistemi di IA ad "osservare norme giuridiche estremamente rigorose" e chiede che siano sempre mantenuti tre profili: 1) la competenza esclusiva dei giudici in tutte le fasi del procedimento penale; 2) l'adozione di decisioni caso per caso; 3) il divieto di utilizzo di IA e tecnologie affini per emanare decisioni giudiziarie.

L'articolo 17 ha ad oggetto invece la spiegabilità, la trasparenza, la tracciabilità e la verifica degli algoritmi. Queste caratteristiche sono, a parere del Parlamento Europeo, imprescindibili per garantire che lo sviluppo, la diffusione e l'utilizzo di sistemi di IA in questo settore rispettino i diritti fondamentali e godano della fiducia dei cittadini. Inoltre, secondo il Parlamento Europeo dovrebbe essere consentito l'acquisto da parte delle autorità giudiziarie e delle forze di polizia solo di

strumenti "che possano essere sottoposti a revisione e siano accessibili … per consentirne la valutazione, la revisione e il controllo". Questi soggetti dovranno poi garantire "trasparenza proattiva" in relazione alle imprese dalle quali acquistano sistemi di IA.

L'articolo 27 rappresenta senz'altro un punto focale della risoluzione, in quanto ha ad oggetto l'utilizzo di tecnologie di *riconoscimento facciale*: secondo il Parlamento Europeo tale attività dovrebbe essere limitata a "finalità chiaramente giustificate nel pieno rispetto dei principi di proporzionalità e di necessità e della legge vigente". In questo articolo il Parlamento Europeo, accogliendo le richieste sempre più numerose provenienti da soggetti della società civile, richiede che venga sancita una *moratoria* sulla diffusione di tali sistemi utilizzati per le attività di contrasto alla criminalità con funzione di "identificazione" (definita all'articolo 25 come la "ricerca della corrispondenza tra una fotografia e un database di immagini"), fintantoché non vengano soddisfatti quattro (ambiziosi) criteri:

1) le norme tecniche non possano essere considerate pienamente conformi con i diritti fondamentali;
2) i risultati ottenuti siano privi di distorsioni e non discriminatori;
3) il quadro giuridico fornisca salvaguardie rigorose contro l'utilizzo improprio e un attento controllo democratico e adeguata vigilanza;
4) vi sia la prova empirica della necessità e proporzionalità della diffusione di tali tecnologie.

Tali criteri non dovranno essere rispettati qualora il sistema sia utilizzato per il riconoscimento di vittime di reati.

Il Parlamento Europeo richiede poi che venga stabilito il divieto permanente di utilizzo negli spazi pubblici dei sistemi di analisi e/o riconoscimento automatici di altre caratteristiche umane quali l'andatura, le impronte digitali, il DNA, la voce e altri segnali biometrici e comportamentali.

Le previsioni della risoluzione in materia di riconoscimento facciale dovranno essere necessariamente coordinate con quanto sancito dall'AI Act,[5] il quale all'articolo 5 inserisce nell'elenco delle pratiche di IA vietate l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto alla criminalità, a meno che e nella misura in cui tale uso sia strettamente necessario per:

[5] *Supra* n. 4.

i. la ricerca mirata di potenziali vittime specifiche di reato, compresi i minori scomparsi;
ii. la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico;
iii. il rilevamento, la localizzazione, l'identificazione o l'azione penale nei confronti di un autore o un sospettato di un reato contemplato dal regime in materia di mandato d'arresto europeo, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno tre anni.

A questo punto della trattazione si deve ricordare che il nostro parlamento parrebbe a prima vista aver colto l'invito del Parlamento Europeo a sancire la moratoria con il decreto Capienze (d.l. del 8 ottobre 2021, n.139, convertito dalla legge 3 dicembre 2021, n.205). Tramite l'articolo 9, commi 9 e ss., del decreto legge, infatti, l'Italia ha sospeso l'installazione e l'utilizzazione di impianti di videosorveglianza con sistemi di riconoscimento facciale basati sull'utilizzo di dati biometrici fino all'entrata in vigore di una disciplina legislativa della materia e comunque non oltre il 31 dicembre 2023.

In realtà, si tratta di un mero abbaglio: la sospensione, infatti, non si applica ai sistemi installati alle autorità competenti per le finalità regolate nel d.l. 51 del 15 maggio 2018 (ossia per le attività di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica). Inoltre, il medesimo decreto Capienze solleva l'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali, nonché di quelle giudiziarie del pubblico ministero, dall'obbligo di consultazione preventiva del Garante per la protezione dei dati personali (previso dall'art. 24, comma 1, lett. b) del d.l. 51/2018).

Ricordiamo da ultimo alcune previsioni importanti della risoluzione, quali la richiesta di divieto di utilizzo di database privati di riconoscimento facciale per le attività di contrasto (art. 28) e l'invito alla Commissione ad intervenire, anche tramite procedura di infrazione, nei confronti di utilizzi di dati biometrici per finalità di applicazione della legge (come nel caso del progetto iBorderCtrl) che portano alla sorveglianza di massa in aree in spazi pubblici.

In conclusione, nonostante la risoluzione costituisca una fonte *non-binding*, rappresenta senz'altro un indizio di quelli che saranno i prossimi passi dell'Unione Europea in questo campo. Essa contiene, difatti, l'invito alla creazione di un quadro regolatorio *forte*. Rimane dunque da chiedersi come tali regole prenderanno forma.