ISSN 1125-856X

Cassazione penale

direttore scientifico **Domenico Carcano**
condirettore **Mario D'Andria**
LXII - Settembre 20**22**, n. **09**

09 2022

estratto

IL SISTEMA DELL'INTELLIGENZA ARTIFICIALE NELLA TRAMA GRAMMATICALE DEL DIRITTO PENALE. DALLA RESPONSABILITÀ UMANA ALLA RESPONSABILITÀ DELLE MACCHINE PENSANTI: UN INATTESO *RETURN TRIP EFFECT*

di Pasquale Troncone

GIUFFRÈ
GIUFFRÈ FRANCIS LEFEBVRE

399 IL SISTEMA DELL'INTELLIGENZA ARTIFICIALE NELLA TRAMA GRAMMATICALE DEL DIRITTO PENALE. DALLA RESPONSABILITÀ UMANA ALLA RESPONSABILITÀ DELLE MACCHINE PENSANTI: UN INATTESO *RETURN TRIP EFFECT*

The artificial intelligence system in the grammatical plot of criminal law. From human responsibility to responsibility of thinking machines: an unexpected trip effect return

L'evoluzione tecnologica degli ultimi anni ha spinto dottrina e giurisprudenza a confrontarsi con la realtà immateriale della Rete e in particolare con la potenzialità lesiva dei mezzi informatici che rendono possibile la gestione dei flussi di dati. L'Unione Europea dopo aver affrontato la sfida normativa della gestione dei dati personali con il Regolamento del 2018 entra in campo questa volta per disciplinare l'attività di una realtà già in essere ma sconosciuta ai molti, quella dell'Intelligenza Artificiale. Il progetto di Regolamento che è stato approvato costituirà una base giuridica del tutto nuova e per molti aspetti originale nella prospettiva diacronica della responsabilità giuridica uomo-macchina. Il diritto penale, così come è accaduto per il trattamento dei dati, non può non interrogarsi sulla necessità/opportunità, in termini di *extrema ratio*, di elaborare fattispecie penali destinate a contenere la forza lesiva dei sistemi di intelligenza artificiale per prevenirne i possibili significativi danni sociali.

The technological evolution of recent years has pushed doctrine and jurisprudence to deal with the intangible reality of the Internet and in particular with the damaging potential of the IT means that make it possible to manage data flows. The European Union, after having faced the regulatory challenge of personal data management with the 2018 Regulation, enters the field this time to regulate the activity of a reality already in existence but unknown to many, that of Artificial Intelligence. The draft Regulation that has been approved will constitute a completely new and in many ways original legal basis in the diachronic perspective of man-machine legal responsibility. Criminal law, as it happened for the processing of data, cannot fail to question the need / opportunity, in terms of last resort, to elaborate criminal cases intended to contain the damaging force of artificial intelligence systems to prevent possible significant damage social.

di **Pasquale Troncone**
Prof. aggr. di Dir. pen. dell'economia - Università di Napoli Federico II

Sommario **1.** L'intelligenza artificiale (IA) chiamata a conciliare le esigenze del mercato con i diritti fondamentali della persona. — **1.1.** Le iniziative normative dell'Unione europea. — **2.** Il Regolamento europeo "COM (2021) 206 final" come base giuridica e indirizzo normativo. — **3.** L'ipotesi del raccordo sistematico e normativo con la disciplina che regola il trattamento dei dati personali. Un bene giuridico già noto. — **4.** La tutela penale dei sistemi di IA trova già un suo profilo in norme punitive della legislazione dell'ordinamento italiano. — **4.1.** Le nuove fonti penali chiamate a regolare l'IA. —

4.2. La criminalizzazione ascendente come criterio di proporzione rispetto allo spettro di intensità del rischio da IA. — **5.** Alla ricerca delle regole sulla responsabilità: il diritto penale ha bisogno dell'uso di IA, ma si impone una tutela penale contro l'abuso dell'IA? Un possibile *return trip effect*. — **5.1.** L'IA come ausilio all'attività di polizia e alla giustizia. La decisione robotica. — **5.2.** La responsabilità penale per l'uso dell'IA: dall'uomo alla macchina e ritorno dalla macchina all'uomo.

1. L'INTELLIGENZA ARTIFICIALE (IA) CHIAMATA A CONCILIARE LE ESIGENZE DEL MERCATO CON I DIRITTI FONDAMENTALI DELLA PERSONA

Il settore dell'informatica giunge progressivamente a lambire sempre nuovi approdi con sviluppi tecnologici che segnano una decisa evoluzione dell'ingegno umano verso nuovi orizzonti e che promettono un vantaggio in termini di benessere e di utilità, ma di cui è difficile cogliere con immediatezza il livello di rischio e responsabilità ad esso correlato [1].

Impedire l'avanzamento anarchico e il pericolo di lesione di interessi per la società e per il singolo sono i nuovi obiettivi del diritto chiamato a intervenire per regolare fenomeni che nascono come scoperte o evoluzioni tecnologiche e finiscono per ripercuotersi come contesti generatori di pericolo per la integrità dei diritti fondamentali della persona [2].

L'Intelligenza Artificiale (IA) è una di quelle frontiere avanzate della moderna tecnologia, certamente in grado di fornire apporti favorevoli al benessere dell'uomo, il cui sviluppo senza regole però potrebbe mettere in pericolo proprio quei vantaggi che si attendono.

Non è un caso che la spiegazione della preoccupata attenzione che le istituzioni comunitarie europee stanno rivolgendo all'uso dell'IA è insita nella capacità di questi nuovi sistemi o macchine intelligenti di pensare come l'uomo, di sostituirsi ad esso per il compimento di tutte quelle azioni che si ripetono e che possono svincolare l'essere umano da semplici adempimenti ciclici. Il tema si pone in termini problematici quando la "macchina per pensare" non si affianca ma si sostituisce all'uomo perché divenuto superfluo, quando lo sovrasta e assume determinazioni svincolate da calcoli di utilità e vantaggi per evitare danni, di cui ogni azione umana si connota. La macchina che si sostituisce all'uomo, che pensa come l'uomo, potrebbe indirizzare la propria meccanica attività verso obiettivi divergenti e distopici da quelli che la ragione umana intende, proprio perché manca quella valutazione alla base fatta di comparazione e controllo precauzionale dei contrapposti effetti [3].

L'avanzamento tecnologico nel settore dell'informatica incede su una strada tracciata dalla necessità di governare la complessità, il contesto multiforme di un mondo integrato, in cui convivono discipline diverse, sensibilità culturali diverse e un diverso modo di intendere

———

[1] A.M. Tuning, *Computing machinery and intelligence*, in *Mind*, 59, 236, p. 433. U. Beck, *La società del rischio. Verso una seconda modernità*, Carocci, Roma, 2000. Per una panoramica sul rapporto tra diritto penale e rischi dello sviluppo tecnologico si veda L. Stortoni, *Angoscia tecnologica ed esorcismo penale*, in *Riv.it. dir. e proc. pen.*, 2004, p. 83; A. Massaro, *Principio di precauzione e diritto penale: nihil novi sub sole?*, in *www.penalecontemporaneo.it*, 9 maggio 2011.

[2] Sul tema il "*Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia*", in *COM (2020) 65 final*, p. 12. Sulla opportunità di individuare regole fisse che possano essere utili per l'introduzione di nuove tecnologie appartenente allo stesso settore G. Finocchiaro, *Riflessioni su diritto e tecnica*, in *Diritto dell'informazione e dell'informatica*, 2012, p. 831. Ampia trattazione della tematica dopo la pubblicazione del Libro bianco è offerta da Aa.Vv., *Intelligenza artificiale tra etica e diritti. Prime riflessioni a seguito del libro bianco dell'unione*, in A.F. Uricchio, G. Riccio, U. Ruffolo (a cura di), Cacucci editore, 2020.

[3] L'efficace definizione è di F. Varanini, *Macchine per pensare. L'informatica come prosecuzione della filosofia con altri mezzi*, Guerini e Associati, 2015.

l'approccio con le varie componenti di una società super-strutturata e indirizzata verso il futuro da una velocissima evoluzione funzionale.

Governare la complessità si impone come un nuovo paradigma che coinvolge inevitabilmente il diritto, il mondo delle regole, l'assetto dei diritti del singolo e del contesto sociale di cui è parte, è un nuovo modo di approcciare la realtà dove la revisione delle logiche cognitive non solo appartengono all'essere umano, ma anche alle macchine che pensano come l'uomo, elaborano procedure e dispensano effetti (4).

Si diceva che le istituzioni dell'Unione Europea sono al lavoro da lungo tempo sul tema, assumendo su di sé il gravoso compito di mettere a punto i contorni di questo nuovo sviluppo tecnologico e di individuarne le coordinate predittive per elaborare adeguate e specifiche regole di governo (5). La preoccupazione da cui ha preso l'avvio questo intenso studio nasce dalla constatazione che l'intelligenza artificiale (IA) è l'abilità di una macchina di mostrare capacità umane quali il ragionamento, l'apprendimento, la pianificazione e la creatività (6). Da qui l'attenzione rivolta all'intelligenza artificiale che permette ai sistemi di capire il proprio ambiente, mettersi in relazione con quello che percepisce, risolvere problemi e agire verso un obiettivo specifico. Il *computer* riceve i dati (già preparati o raccolti tramite sensori, come una videocamera), li processa e risponde. Non solo. È in grado successivamente di evitare passaggi che ha già elaborato e fatto propri, adattando il suo futuro agire agli effetti di attività precedenti, orientando il suo comportamento in piena autonomia.

Questa "maturità" destinata ad essere acquisita progressivamente mette a nudo l'enorme potenzialità dei sistemi IA di sostituirsi all'operatore umano, di pensare al suo posto, di ottenere sul campo un'indipendenza che potrebbe travolgere mano a mano la necessità del ponderare dell'uomo, per imporre il meccanico processo di dati e azioni svolto in maniera intelligente. Non basta, perché la punta più avanzata al momento è costituita dalla c.d. polizia predittiva che consente la raccolta di enormi quantità di dati biometrici negli spazi pubblici, in grado di invadere in maniera imponente la riservatezza delle persone attraverso la catalogazione di categorie pericolose per la sicurezza sociale nonché il riconoscimento fotografico dei soggetti da individuare e vigilare (7).

Naturalmente il tema che una ipotizzabile "tecnologia difensiva" deve affrontare contro derive anarchiche è quello del controllo etico sulla macchina che tenderà sempre di più ad acquisire indipendenza e autonomia di giudizio e di azione (8). Il controllo deve tuttavia nascere dalla previa individuazione degli obiettivi che allo stesso tempo non possono essere eccessi-

———

(4) S. Aleo - G. Pica, *Sistemi giuridici, complessità @comunicazione*, Bonanno Editore, 2009, p. 56 e p. 81.

(5) La preoccupazione che ha mosso in primo luogo le istituzioni nazionali ed europee nasce per l'uso dell'IA nel settore della giustizia, come dimostrato dalla "*Carta etica europea sull'utilizzo dell'intelligenza artificiali nei sistemi giudiziari e negli ambiti connessi*", adottata dalla Commissione europea a Strasburgo il 3-4 dicembre 2018. S. Quattrocolo, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, in *www.lalegislazionepenale.eu*, 18 dicembre 2018. V. Manes, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in Studi in onore di Lucio Monaco, in A. Bondi, G. Fiandaca, G.P. Fletcher, G. Marra, A.M. Stile, C. Roxin, K. Volk (a cura di), Urbino University Press, 2020, p. 687.

(6) Sull'origine dei sistemi di intelligenza artificiale si veda G.F. Italiano - E. Prati, *Storia, tassonomia e sfide future dell'intelligenza artificiale*, in Aa.Vv., *Intelligenza artificiale. Politica, economia, diritto, tecnologia*, di Paola Severino (a cura) Luiss U.P., Roma, 2022, p. 57.

(7) A. Bonfanti, Big data *e polizia predittiva: riflessioni in tema di protezione del diritto alla* privacy *e dei dati personali*, in *MediaLaws*, 24 ottobre 2018.

(8) Ricche informazioni sono contenute nello *Statuto Etico e Giuridico dell'IA*, Fondazione Leonardo, in *www.civiltadellemacchine.it*.

vamente restrittivi e impedire una imponente riduzione della potenzialità operativa della macchina pensante [9].

1.1. Le iniziative normative dell'Unione europea

Intanto l'Unione Europea mette in campo prima di tutto una serie di importanti documenti per conciliare il sistema dell'IA con il mercato interno, avvedendosi che il disegno continentale del rispetto della persona umana e della sua dignità può essere realizzato soltanto se alla base si concilia la finalità dello sviluppo tecnologico con il rispetto dei diritti fondamentali della persona e il principio di non discriminazione che sono l'essenza stessa della scelta istitutiva dell'Unione Europea [10].

Il mandato normativo che ne consegue è fissato nella premessa al Regolamento *COM (2021) 206 final*, fonte direttamente applicabile agli ordinamenti interni degli stati membri: "L'uso dell'intelligenza artificiale, garantendo un miglioramento delle previsioni, l'ottimizzazione delle operazioni e dell'assegnazione delle risorse e la personalizzazione dell'erogazione di servizi, può contribuire al conseguimento di risultati vantaggiosi dal punto di vista sociale e ambientale nonché fornire vantaggi competitivi fondamentali alle imprese e all'economia europea. Tale azione è particolarmente necessaria in settori ad alto impatto, tra i quali figurano quelli dei cambiamenti climatici, dell'ambiente e della sanità, il settore pubblico, la finanza, la mobilità, gli affari interni e l'agricoltura".

La linea di indirizzo appare a questo punto evidente, si è assunto una direttrice divergente rispetto al passato quando le finalità delle Comunità europee ruotavano soltanto intorno al mercato e al profitto: "La presente proposta impone alcune restrizioni alla libertà d'impresa (articolo 16) e alla libertà delle arti e delle scienze (articolo 13) al fine di assicurare il rispetto di motivi imperativi d'interesse pubblico quali la salute, la sicurezza, la tutela dei consumatori e la protezione di altri diritti fondamentali ("innovazione responsabile") nel momento in cui si diffonde e si utilizza una tecnologia di IA. Tali restrizioni sono proporzionate e limitate al minimo necessario per prevenire e attenuare rischi gravi per la sicurezza e probabili violazioni dei diritti fondamentali" [11].

La prima assoluta novità si coglie nella nuova visione culturale che l'Europa intende garantirsi, affrancandosi dalle ragioni storiche per cui nasce: abbandonare la visione che vedeva l'unità dei paesi europei radicata sulle esigenze di un mercato economico e di una moneta comune, per aprirsi ad una visione umanistica che veda l'uomo al centro delle nuove politiche continentali. Soltanto in questa nuova prospettiva ci si propone di conciliare le esigenze dell'uomo attraverso la regolazione dei mercati e il controllo su tutti meccanismi che ne possano favorire la crescita, la disciplina, sempre e soltanto nel rispetto dei diritti fondamentali della persona umana [12].

———

[9] F. Basile, *Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine*, in *www.dirittopenaleuomo.org*, 29 settembre 2019.

[10] AA.VV., *Intelligenza artificiale e diritti della persona*, di D. Buzzelli e M. Palazzo (a cura), Pacini Giuridica, 2022.

[11] Al punto 3.5. "*Diritti fondamentali*" della proposta di Regolamento. Sul punto va ricordato il recente Rapporto pubblicato il 27 ottobre 2021da ENISA (*Network and Information Security Agency*) sugli attacchi informatici subiti negli ultimi mesi da Istituzioni ed Enti europei nonché il furto di archivi digitalizzati.

[12] Al punto 15 del Regolamento: "L'intelligenza artificiale presenta, accanto a molti utilizzi benefici, la possibilità di essere utilizzata impropriamente e di fornire strumenti nuovi e potenti per pratiche di manipolazione, sfruttamento

Questo cambio di strategia punta ad armonizzare la crescita e il benessere con la tirannia dei mercati e, del resto, vuole testimoniare l'integrazione dei principi che guidarono la stesura dei Trattati fondativi dell'Unione con la Convezione Europea dei Diritti dell'Uomo. Solo a queste condizioni l'Europa può conquistare la meta di una integrazione di sistemi sociali e giuridici diversi e l'uniformità delle determinazioni, evitando discriminazioni sociali ed economiche.

La pandemia da *COVID-19* ha messo in evidenza che esistono strade alternative alle decisioni autoritative in chiave unicamente del profitto, lanciando una idea di crescita sociale ed economica che parta dalle esigenze delle persone e non dalle esigenze dei mercati.

In definitiva, qualunque *policy* messa sul terreno per favorire lo sviluppo deve essere temperata da scelte etiche che riportino i sistemi ai bisogni della persona, partendo proprio dalla previsione di regole e norme che stabiliscano un corretto vincolo dei fini [13].

L'intelligenza artificiale non può essere, dunque, svincolata da questo modello sistematico, perché la sua esistenza è fondata sulla raccolta e l'accumulo di dati personali e la sua operatività intanto esiste se esistono i dati che devono essere elaborati e trattati [14]. Senza dati la macchina pensante non ha il carburante per attivarsi, non ha lo scopo che ne connota l'operatività e l'utilità.

I dati personali sono, infatti, il nuovo mercato digitale degli stati, un mercato alimentato da miliardi di dati che quotidianamente si accumulano per effetto della presenza degli utenti sulla Rete e che incessantemente continuano a incrementare i serbatoi di dati [15]. Questi serbatoi – archivi informatizzati indicizzati – diventano il nuovo prodotto offerto sul mercato che genera profitto semplicemente perchè il trattamento di quei dati è indispensabile all'impresa. Basta osservare quanti dati bio-medici sono stati forniti al mercato digitale durante la pandemia e che saranno utilizzati dalle case farmaceutiche per mettere a punto nuovi vaccini e farmaci. Peraltro, il recente recepimento della Direttiva UE 2019/770 avvenuta da parte del nostro Paese con l'inserimento dall'art. 135-*octies* all'art. 135-*vicies ter* nel Codice del consumo d.lg. n. 206/2005 ha stabilito la monetizzazione dei dati digitali, in modo che oggi sono considerati vera e propria moneta, utile per acquistare contenuti e servizi digitali [16].

Tutto questo ampio contesto in cui interagiscono flussi ininterrotti di dati e che attraverso la macchina dell'intelligenza artificiale vengono rielaborati e finalizzati, attende a questo punto una disciplina che ne regoli la gestione e che assicuri la puntuale protezione degli interessati.

———

e controllo sociale. Tali pratiche sono particolarmente dannose e dovrebbero essere vietate poiché contraddicono i valori dell'Unione relativi al rispetto della dignità umana, della libertà, dell'uguaglianza, della democrazia e dello Stato di diritto e dei diritti fondamentali dell'Unione, compresi il diritto alla non discriminazione, alla protezione dei dati e della vita privata e i diritti dei minori".

[13] L. Floridi, *Agere sine intelligere. L'intelligenza artificiale come nuova forma di agire e i suoi problemi etici*, in L. Floridi - F. Cabitza, *Intelligenza artificiale. L'uso delle nuove macchine*, Bompiani, 2021, p. 115.

[14] Aa.Vv., *Intelligenza artificiale, protezione dei dati personali e regolazione*, di F. Pizzetti (a cura), Giappichelli, Torino, 2018. G. Finocchiaro, *Intelligenza Artificiale e protezione dei dati personali*, in *Giur. it.*, 2019, p. 1670.

[15] A. Mantelero, *Report on Artificial Intelligence. Artificial Intelligence and Data Protection: Challenges and Possible Remedies*, in *Commissione consultiva della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*, 25 gennaio 2019.

[16] V. Ricciuto, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Diritto dell'informazione e dell'informatica*, 2018, p. 689.

2. IL REGOLAMENTO EUROPEO "COM (2021) 206 FINAL" COME BASE GIURIDICA E INDIRIZZO NORMATIVO

Il sistema delle fonti europee del diritto segnala che qualunque disciplina ad essa pertinente, di cui dovrà farsi carico il legislatore interno allo stato nazionale, non può prescindere da una "base giuridica" che ne forma il movente e che non manca in questo caso: "La base giuridica della proposta è costituita innanzitutto dall'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE), che prevede l'adozione di misure destinate ad assicurare l'instaurazione ed il funzionamento del mercato interno" [17].

L'assetto delle regole del diritto, con l'avvento delle discipline europee dotate di immediata forza di legge, insegna che in un quadro sistematico di policentrismo delle fonti la base giuridica molto spesso è da rintracciare in testi normativi diversi. In questo caso il legislatore eurounitario, come è già avvenuto con il GDPR, preferisce introdurre la complessa disciplina con un "Regolamento" di immediata efficacia negli stati membri e non con una "Direttiva", anche al fine di vincolare il legislatore nazionale al carattere di uniformità e coerenza normativa del settore.

Il 21 aprile 2021 è stato approvata la 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" che, dopo una lunga premessa descrittiva e la fissazione di coordinate metodologiche, fornisce un complesso articolato disciplinare dove all'art. 1 ne indica la *mission* giuridica, vale a dire le: "regole armonizzate per l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di intelligenza artificiale ("sistemi di IA") nell'Unione".

Il Regolamento ha lo scopo di connettere il mercato digitale delle informazioni e dei dati personali, vale a dire il patrimonio informativo che costituisce la riservatezza della persona, con i meccanismi operativi dell'IA, allo scopo di stabilire la natura delle relazioni e le regole di diligenza per un corretto comportamento da assumere, ossia il livello di tutela da garantire, quando i dati sono trattati dai sistemi di IA [18]. Pertanto, la tutela della persona umana discende direttamente dall'esigenza di mettere a punto la macchina dell'IA, poiché l'oggetto delle sue operazioni sono agevolmente identificabili nel concetto del trattamento di dati personali, oltre naturalmente di altri dati che non hanno alcuna connotazione relativa alla persona umana e che, comunque, non possono sfuggire alla base giuridica della materia. Solo in questa prospettiva, infatti, va considerato il profilo di maggiore rilevanza del Regolamento che, nel proposito di coniugare il livello operativo della macchina dell'IA con i dati che costituiscono il suo necessario patrimonio informativo su cui lavorare, fissa le regole giuridiche nel suo disciplinare.

Come sempre nelle fonti europee viene fornito un corredo di "Definizioni" per assicurare uniformità interpretativa al testo. Anche in questo caso il legislatore sovranazionale fornisce la definizione normativa, precettiva, del "sistema di intelligenza artificiale" (sistema di IA), come di: "*un software* sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali

———

[17] Punto 2.1 del Regolamento "*Base giuridica*".

[18] Sulle problematiche legate al controllo del diritto sullo sviluppo tecnologico, si rinvia a G. Marinucci, *Innovazioni tecnologiche e scoperte scientifiche: costi e tempi di adeguamento delle regole di diligenza*, in *Riv. it. dir. e proc. pen.*, 2005, p. 29.

contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono" [19].

A questo punto si apre il tema dei settori in cui l'IA suscita interesse, per individuare quali tipi di applicazione potrà avere e, soprattutto, la regolazione giuridica delle sue procedure e dei suoi effetti. Il mondo del diritto è chiamato prima di ogni altra cosa ad interrogarsi sui profili e la natura della responsabilità per l'uso dei sistemi di IA e nella stessa misura scendono sul terreno le regole del diritto civile e del diritto penale.

Occorre infatti precisare che il diritto penale nutre un particolare interesse per la materia dell'IA: *a*) come strumento predittivo di biometria in remoto per prevenire e contrastare episodi criminali, anche individuando gli autori preventivamente o successivamente alla commissione di un reato, attraverso immagini o riconoscimento vocale [20]; *b*) per assumere la funzione decisoria surrogando la decisione giudiziaria del magistrato umano; *c*) per ipotizzare fattispecie di reato che puniscano la violazione delle regole di correttezza nell'uso del sistema intelligente per i precedenti impieghi [21].

Prima ancora di individuare le possibili condotte lesive e i rischi consentiti nell'uso dell'IA e strutturare specifiche ipotesi di reato, la trama metodologica del diritto penale impone di verificare se esiste un bene o un interesse giuridico importante che la legge penale possa prendere in carico, rivolto alla tutela di interessi nuovi ed emergenti, cui si ritiene indispensabile il presidio di una norma punitiva in termini di *extrema ratio*.

Oggi la base giuridica del diritto dell'Unione Europea, così come è accaduto per il trattamento e la circolazione dei dati personali, mette a disposizione del giurista, e del penalista in particolare, sufficienti elementi di identificazione di quel bisogno di pena che deve accompagnare qualunque norma punitiva di natura penale. Peraltro, la materia dell'IA attinge ad un settore già noto alla legislazione penale italiana, quella del Codice della *privacy* n. 196/2013, per cui va individuata la base giuridica nell'ambito del Regolamento sull'AI per ravvisare l'opportunità anche in questo caso di una tutela penale da parte dello stato nazionale.

Ebbene in questa indagine di tipo ricognitivo il primo avamposto che può favorire lo scopo teleologico si rinviene nell'art. 5 del Titolo II "Pratiche di intelligenza artificiale vietate", in cui già il legislatore euro-unitario ha ravvisato la necessità di protezione, segnalando l'esigenza di un intervento in termini di prevenzione, oltre che di repressione, per evitare conseguenze lesive. I sistemi ad alto rischio sono quelli indicati all'art. 7 che riguardano i rischi di danno alla salute, alla sicurezza o per la lesione di diritti fondamentali. E poi ancora l'intero Titolo III "Sistemi di IA ad alto rischio" dedicato ai criteri di individuazione e poi della gestione del rischio. Orbene, in queste norme, in particolare l'art. 10 "Dati e *governance* dei dati" a seguire, sono riportate proprio operazioni che riguardano il trattamento dei dati, tra cui i dati personali.

———

[19] Per le diverse definizione dell'IA succedutesi nel tempo cfr. Malaschini A., *Regolare l'intelligenza artificiale*, in Aa.Vv., *Intelligenza artificiale*, cit., p. 105. Occorre aggiungere che per la prima volta l'IA è divenuta oggetto di una pronuncia giurisprudenziale, in cui viene adottata una sua specifica definizione, in Consiglio di Stato, Sez. III, Sent. n. 7891 del 25 novembre 2021: "In questo caso l'algoritmo contempla meccanismi di *machine learnig* e crea un sistema che non si limita solo ad applicare le regole *sofware* e i parametri preimpostati (come fa invece l'algoritmo "tradizionale") ma, al contrario, elabora costantemente nuovi criteri di inferenza tra dati e assume decisioni efficienti sulla base di tali elaborazioni, secondo un processo di apprendimento automatico", in *www.altalex.it*.

[20] L. Saponaro, *Le nuove frontiere tecnologiche dell'individuazione personale*, in *Arch. pen.*, n. 1, 2022.

[21] Sul punto anche P. Severino, *Intelligenza artificiale e diritto penale*, in Ugo Ruffolo (a cura di), Aa.Vv., *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, 2020, p. 536.

Le interrelazione tra la materia dell'IA e quella del trattamento di dati trova, infatti, una sua più precisa sottolineatura con la lett. *f*) dell'art. 17 "Sistema di gestione della qualità": "i sistemi e le procedure per la gestione dei dati, compresa la raccolta, l'analisi, l'etichettatura, l'archiviazione, la filtrazione, l'estrazione, l'aggregazione, la conservazione dei dati e qualsiasi altra operazione riguardante i dati effettuata prima e ai fini dell'immissione sul mercato o della messa in servizio di sistemi di IA ad alto rischio".

Intanto, il n. 2 dell'art. 14 "*Sorveglianza umana*" stabilisce quale tipo di controllo di tipo preventivo deve essere eseguito sull'attività dell'IA, assegnando rilevanza giuridica a quell'interesse destinato ad assurgere a oggetto di protezione penale: "La sorveglianza umana mira a prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali che possono emergere quando un sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile, in particolare quando tali rischi persistono nonostante l'applicazione di altri requisiti di cui al presente capo".

Tuttavia, la norma più importante che emerge dalla complessa disciplina e che determina un raccordo diretto tra i testi del Regolamento europeo sul trattamento dei dati personali (il *GDPR*) e il Regolamento sull'IA è senza dubbio quella che stabilisce, con l'art. 70 "*Riservatezza*" in maniera espressa, la tutela della riservatezza delle operazioni compiute e dei dati trattati e circolati.

3. L'IPOTESI DEL RACCORDO SISTEMATICO E NORMATIVO CON LA DISCIPLINA CHE REGOLA IL TRATTAMENTO DEI DATI PERSONALI. UN BENE GIURIDICO GIÀ NOTO

L'art. 70, si è detto, stabilisce la centralità del bene giuridico "riservatezza personale" che, pur autonomamente emerso nel diritto nazionale italiano – sebbene con molto ritardo –, assume in misura sempre più delineata la rilevanza nella base giuridica sovranazionale, tanto più importante in quanto destinata a imporre criteri di uniformità a tutti gli stati dell'Unione [22].

Ormai la tutela dei dati personali ha guadagnato anche una dimensione costituzionale in alcuni Paesi dell'Unione e nelle Carte fondamentali sovranazionali, ampliando decisamente sia la base giuridica di riferimento sia il contenuto di valore ad esso connesso, come è dato leggere all'art. 8 della Carta EDU: "Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza". A questa si affianca la Costituzione spagnola che al quarto comma dell'art. 18 stabilisce che: "La ley limitarà el uso de la informatica *para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*" [23]; nonché la Costituzione irlandese che con l'art. 10 impone al legislatore ordinario di emanare norme a tutela della *privacy* [24].

———

[22] Ci sia consentito sul tema citare P. Troncone, *La tutela penale della riservatezza e dei dati personali. Profili dommatici e nuovi approdi normativi*", ESI, 2020.

[23] Art. 18, comma IV: "*La legge limita l'utilizzazione dell'informatica al fine di garantire l'onore, l'intimità personale e familiare dei cittadini e il pieno esercizio dei loro diritti*". Nell'ambito delle fonti legislative ordinarie dell'ordinamento spagnolo esiste una regolamentazione specifica, sul punto cfr. M. Losano, *Le norme sulla violazione della riservatezza nel nuovo codice penale spagnolo*, in *Dir. inform.*, 1996, I, p. 535 ss.

[24] Su tutti gli aspetti relativi all'adozione di un codice per il trattamento dei dati personali in Spagna, si veda A.I. Herran Ortiz, *El derecho a la intimidad en la nueva Ley Organica de Proteccion de Datos Personales*, Ed. Dykinson, Madrid, 2002. C. Russo, *Commento all'art. 8 § 1*, in *La Convention européenne des droits de l'homme. Commentaire article par article*, a cura di L.E. Petitti, E. Decaux, P.H. Imbert, Paris, Economica, 1995, p. 355. Si veda in proposito F.

Peraltro, la Carta di Nizza, pur non rivestendo i caratteri di uno strumento giuridico in senso stretto, poiché non possiede la forma del "Trattato", con il c.d. "Trattato di Lisbona", sottoscritta il 13 dicembre 2007 ed entrato in vigore il I dicembre 2009, assume una valenza significativa, sotto il profilo dell'uniformità sovranazionale della base giuridica, con l'art. 8 "Protezione dei diritti di carattere personale": "1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".

Da queste espresse previsioni occorre trarre una riflessione di ordine sistematico che riconosca un raccordo normativo tra le due materie, il GDPR e il progetto di Regolamento dell'IA, che, sebbene oggi compaiano sulla scena con distinti provvedimenti regolamentari e autonome basi giuridiche, in realtà suggeriscono di trattare la vasta area tematica in maniera integrata secondo i criteri direttivi di interpretazione sistematica.

Ad avvalorare in questo senso un quadro normativo che prelude alla nascita di un vero e proprio sistema contribuisce la previsione dell'art. 63 del Regolamento sull'IA "Vigilanza del mercato e controllo dei sistemi di IA nel mercato dell'Unione" che al punto 5 stabilisce: "Per i sistemi di IA elencati al punto 1, lettera *a*), nella misura in cui tali sistemi sono utilizzati a fini di attività di contrasto, e ai punti 6 e 7 dell'allegato III, gli Stati membri designano come autorità di vigilanza del mercato ai fini del presente regolamento le autorità di controllo competenti per la protezione dei dati a norma della direttiva (UE) 2016/680 o del regolamento (CE) n. 2016/679 o le autorità nazionali competenti che controllano le attività delle autorità di contrasto o delle autorità competenti in materia di immigrazione o di asilo che mettono in servizio o usano tali sistemi"; e poi con il successivo punto 6 prevede: "Nei casi in cui le istituzioni, le agenzie e gli organismi dell'Unione rientrano nell'ambito di applicazione del presente regolamento, il Garante europeo della protezione dei dati agisce in qualità di autorità di vigilanza del mercato".

Orbene, questa forma di rispetto della riservatezza personale emerge in realtà in una forma indiretta e inconsueta, in un contesto nel quale l'IA sarebbe chiamata a svolgere semplicemente una serie di attività computazionali che si risolvono in mere operazioni informatiche.

Ma così non è, perché i due spazi operativi trovano una forma di raccordo indiretto, ma estremamente significativo, proprio per il fatto che le operazioni di IA, in definitiva, finiscono per trattare anche dati personali oltre che quelli tecnici, imponendosi quel livello di discrezione e di protezione che il GDPR appresta all'uso e alla gestione dei dati personali.

4. LA TUTELA PENALE DEI SISTEMI DI IA TROVA GIÀ UN SUO PROFILO IN NORME PUNITIVE DELLA LEGISLAZIONE DELL'ORDINAMENTO ITALIANO

Un'ampia ricognizione svolta sugli obblighi normativi di tutela che emergono dal testo della proposta di Regolamento europeo sull'IA suggerisce al legislatore nazionale di introdurre norme punitive essenzialmente, ma non esclusivamente, orientate al campo del diritto ammi-

———

Donati, *Protezione dei dati di carattere personale*, in *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione Europea*, a cura di R. Bifulco, M. Cartabia e A. Celotto, Il Mulino, 2001, p. 83 ss.

nistrativo munite di sanzioni pecuniarie. Tuttavia, come è accaduto con il GDPR europeo in materia di trattamento di dati, non viene esclusa con l'art. 71 la possibilità che lo stato nazionale possa adottare norme penali.

Prima di affrontare il tema dello spettro sanzionatorio che in termini di *extrema ratio* potrebbe spaziare dalle infrazioni amministrative fino a fattispecie di reato a seguito della libera determinazione degli ordinamenti nazionali, è opportuno aprire l'indagine sul quadro sistematico della nostra legislazione interna per verificare quali interazioni potrebbero esserci tra il provvedimento normativo che regola l'IA e l'ampia disciplina di norme punitive già esistenti.

Avere individuato in premessa un nuovo bene giuridico di categoria radicato su una nuova base giuridica, cui valutare se e in quale misura apprestare tutela, è stato utile per accertare se vi sono le condizioni per ipotizzare una tutela penale ulteriore a quella espressa già in altri ambiti disciplinari. In effetti, la materia dell'IA viene ad intersecare due precise fonti del diritto che nel nostro ordinamento interno già sono chiamate a punire fatti lesivi di beni giuridici appartenenti, se non con evidenza alla medesima categoria, a situazioni molto vicine a quelle che si trovano disciplinati dall'IA.

In questo caso vanno tenute nettamente distinte le vicende che investono i dati trattati dalla macchina dell'IA e quelle che riguardano i mezzi, le piattaforme, i supporti tecnologici per compiere il trattamento, nella doppia dimensione dei sistemi di *hardware* e *software*. Dunque, prima di tutto il Codice della *privacy* nella sua parte relativa alla previsione di norme penali e poi la diffusa disciplina penalistica dei reati informatici appartenente allo specifico settore del codice penale.

In questi termini, a ben vedere, l'ampia gamma dei suggerimenti che fornisce la proposta di Regolamento, circa l'attivazione di una risposta sanzionatoria per la violazione di specifici obblighi puntualmente prescritti, sono già in parte oggetto della disciplina di norme penali interne. Per cui il legislatore nazionale ha già risolto anticipatamente l'esigenza del bisogno di pena, in quanto ha già individuato fatti che assumono rilevanza tale da meritare la censura con la sanzione penale.

4.1. Le nuove fonti penali chiamate a regolare l'IA

Da un punto di vista metodologico l'intervento legislativo dovrà preliminarmente operare una scelta: inserire nuove norme punitive – che siano amministrative o penali – nel corpo dei provvedimenti legislativi preesistenti ovvero il Parlamento italiano, attraverso una legge di delegazione europea, dovrà conferire al Governo il potere di emanare un provvedimento autonomo come specchio del Regolamento europeo?

Seguendo le coordinate concettuali della riserva di codice dell'art. 3-*bis* c.p. la scelta più opportuna sarebbe quella di implementare nuove norme nella legislazione vigente, evitando una nuova fonte legislativa destinata a duplicare molte delle norme esistenti, con nodi interpretativi da risolvere attraverso il criterio di specialità dell'art. 15 c.p. Questo tipo di scelta, da privilegiare, risponderebbe anche a una lettura sistematica di vicende normative che ruotano attorno a medesimi beni giuridici, confermando quella uniformità applicativa che la sede giurisprudenziale da sempre reclama. D'altronde l'unità sistematica, fondata su coordinate di tipo assiologico e logico, risolvono non solo questioni legate all'antinomia normativa, ma

soprattutto prevengono conflitti sul piano della determinatezza che si affacciano sul terreno dell'interpretazione quando si interviene più volte sugli stessi beni giuridici [25].

Peraltro, non è assimilabile l'esperienza dell'introiezione del futuro Regolamento europeo dell'IA a quello del GDPR nell'ordinamento italiano, in quanto già esisteva il Codice della *privacy* come specifica fonte di settore.

Riconoscere e rispettare l'unità sistematica in questo caso sarebbe un grande vantaggio anche per le ricadute processuali che la materia presenta, sia per i provvedimenti di carattere cautelare sia per la fase delle indagini preliminari che, come nel caso del trattamento di dati, vede appunto la presenza oltre che del PM anche del Garante della *privacy*. Va, infatti, precisato che anche in questa materia emerge con chiarezza la figura del Garante della *privacy* europeo e per gli stati nazionali la corrispondente Autorità indipendente, a conferma del fatto che la materia dell'IA è la punta più avanzata di un settore giuridico che gli ordinamenti già conoscono e le legislazioni nazionali hanno già implementato [26].

Non vi è dubbio che il possibile ricorso alla sanzione penale vede preliminarmente sciolto il suo nodo, dal momento che esistono già nella nostra legislazione penale nazionale ben due diversi settori normativi che incrociano la materia dell'IA, per cui le relative fattispecie di reato ivi previste sono già materia di legislazione preesistente. Ed infatti, il disvalore di talune condotte di trattamento dei dati risulta già ricompreso in fattispecie incriminatrici vigenti, si pensi all'ampia appendice penalistica al Codice della *privacy* a partire dall'art. 167 Cdp. Sarebbe, dunque, un fuor d'opera ipotizzare nuove figure di reato che andrebbero deprecabilmente a duplicare quelle esistenti, con grave asincronia sul principio di specialità. Del resto, il proposito di completare la tutela per talune circostanze e specificità non ancora previste potrebbe essere ottenuto semplicemente integrandone i precetti.

Posto in premessa che la materia merita rilevanza penale, occorrerà enucleare quegli obblighi e divieti contenuti nel futuro Regolamento dell'IA che possono costituire oggetto di nuove figure di reato, sottolineando il rispetto del criterio di proporzionalità tra la rilevanza dell'interesse da proteggere e l'adeguatezza della pena da prevedere come conseguenza. Il canone di proporzionalità deve giocare in questo caso un duplice ruolo: da un lato riconoscere la necessità di un intervento forte da parte dell'ordinamento con la previsione di una fattispecie di reato e di una pena; dall'altro individuare quella misura della pena adeguata che possa

———

[25] AA.VV., *Il sistema penale ai confini delle hard sciences. Percorsi epistemologici tra neurosceinze e intelligenza artificiale*, di F. Basile, M. Caterini, S. Romano, (a cura), Pacini Giuridica, 2021.

[26] All'art. 63 della proposta di Regolamento: "5. Per i sistemi di IA elencati al punto 1, lettera *a*), nella misura in cui tali sistemi sono utilizzati a fini di attività di contrasto, e ai punti 6 e 7 dell'allegato III, gli Stati membri designano come autorità di vigilanza del mercato ai fini del presente regolamento le autorità di controllo competenti per la protezione dei dati a norma della direttiva (UE) 2016/680 o del regolamento (CE) n. 2016/679 o le autorità nazionali competenti che controllano le attività delle autorità di contrasto o delle autorità competenti in materia di immigrazione o di asilo che mettono in servizio o usano tali sistemi". Peraltro, con il Piano nazionale di ripresa e resilienza (PNRR) il Governo italiano ha stanziato la quota del 27% delle risorse da destinare all'AI e per questo si intravede una soluzione normativa che affidi al Garante della *privacy* italiano la competenza anche sulle operazioni di AI, integrando in questo senso la disciplina regolamentare dell'Autorità indipendente. Sul tema G. Borgia, *Profili sistematici delle tecnologie di riconoscimento facciale automatizzato, anche alla luce dei futuribili sviluppi normativi sul fronte eurounitario*, in *www.lalegislazionepenale.eu*, 11 dicembre 2021.

conciliare istanze di tipo preventivo con quelle rieducative e di integrazione sociale, secondo la nostra prospettiva costituzionale interna [27].

4.2. La criminalizzazione ascendente come criterio di proporzione rispetto allo spettro di intensità del rischio da IA

L'intervento di criminalizzazione in termini di *extrema ratio* e di proporzionalità della risposta sanzionatoria trova i suoi immediati referenti qualificativi nei diversi livelli di rischio che sono espressamente segnalati dalla proposta di Regolamento europeo e che pone in evidenza la particolare potenza impattante di questa nuova tecnologia.

Nella scala di valore segnalata dal testo si presenta per prima la categoria delle pratiche "assolutamente vietate", delineate dal c.d. "rischio assoluto o inaccettabile" che impedisce qualsiasi pratica di IA in specifici settori tassativamente indicati dall'art. 5, perché concretizzano più di ogni altra occasione di discriminazione personale e sociale. Basta solo segnalare l'uso di tecniche subliminali, l'uso da parte di pubbliche autorità di sistemi che stabiliscano la differenza tra gruppi di persone o individuino i soggetti particolarmente vulnerabili differenziandoli dal resto, l'identificazione biometrica indiscriminata a distanza e in tempo reale. Questa pratica in particolare appare come la più invasiva e incontrollabile in assoluto, poiché consente di scandagliare immagini e suoni per risalire alla identificazione di persone effettuando una selezione tra tutti coloro che entrano nel raggio di azione dei sistemi di telerilevamento. Tuttavia, il Regolamento consente eccezionalmente l'uso di questi processi per ragioni di polizia o per rintracciare persone scomparse, sempre che il loro uso sia limitato nel tempo e a porzioni di territorio.

La giurisprudenza convenzionale a questo proposito ha posto dei punti fermi insuperabili, allorché ha stabilito che tutte le forme di indagine invasiva devono trovare alla base della loro operatività un provvedimento del giudice che le autorizzi – si pensi alla *data retention* e all'uso dei tabulati telefonici oltre alle intercettazioni telefoniche e ambientali –, impedendo qualunque accesso per semplici ricognizioni di polizia o di prevenzione.

Seguono poi le applicazioni consentite anche se connotate da un rischio "alto ma accettabile" previste all'art. 6 e ss. In questo ambito vi sono anche operazioni con rischio "sensibile ma minore e controllabile".

Infine, sono previste le operazioni con "rischio nullo" per operazioni tecnicamente semplici e del tutto innocue, tra le quali rientra la semplice manutenzione del sistema di IA.

La scala di valore del rischio fissata da specifiche ipotesi normative semplifica il lavoro del legislatore che volesse ravvisare la necessità di approntare una protezione di natura penale a questo settore così sensibile. Così come si era auspicato dopo il GDPR occorre affidarsi a scelte sanzionatorie in grado di esercitare la giusta dissuasione percorrendo una strada del tutto opposta a opzioni di tipo retributivo o intimidative, tipiche della prevenzione generale negativa.

Il settore dell'IA suggerisce di conciliare in maniera bilanciata le ragioni della punizione (o la sanzione derivante da istituti di diversione processuale) con l'approccio precauzionale che le innumerevoli operazioni di IA richiedono, valutando l'opportunità di introdurre un catalogo sanzionatorio che tenga conto di meccanismi di recupero sociale attraverso strumenti norma-

———

[27] Sulla proporzionalità, per tutti F. Viganò, *La proporzionalità della pena. Profili di diritto penale e costituzionale*, Giappichelli, 2021.

tivi di sospensione della pena condizionati da una prova di affidabilità della persona e dei suoi contesti di appartenenza [28].

5. ALLA RICERCA DELLE REGOLE SULLA RESPONSABILITÀ: IL DIRITTO PENALE HA BISOGNO DELL'USO DI IA, MA SI IMPONE UNA TUTELA PENALE CONTRO L'ABUSO DELL'IA? UN POSSIBILE *RETURN TRIP EFFECT*

Non vi è dubbio che oggi la giustizia penale ha necessità di mezzi tecnologici che siano in grado di garantire il controllo della criminalità, di prevenire reati, di individuare i responsabili e anche di vigilare sulle misure e le pene scontate in libertà da persone condannate (si pensi all'uso del braccialetto elettronico) [29].

5.1. L'IA come ausilio all'attività di polizia e alla giustizia. La decisione robotica

Sul punto in data 6 ottobre 2021 il Parlamento europeo ha approvato un documento particolarmente importante "L'intelligenza artificiale nel diritto penale e il suo utilizzo da parte delle autorità di polizia e giudiziarie in ambito penale" che segna il punto di inizio del rapporto tra la giustizia penale e l'istituzionalizzazione delle attività riconducibili all'IA.

La ricaduta di questo provvedimento sui diritti della persona e in particolare i diritti di libertà non può essere sottovalutata. Si pensi all'applicazione dell'IA per l'adozione delle misure di prevenzione personale, dove le operazioni di IA possono costituire l'unico materiale indiziario per elaborare il giudizio di pericolosità sociale del prevenuto, con tutti i rischi connessi all'uso di algoritmi predittivi [30].

Si tratta di nuove forme di vigilanza e di nuovi approcci di indagine, dove non deve mai venir meno l'apporto ragionato e ragionevole dell'uomo che potrebbe non essere più un giudice umano ma un operatore tecnico [31].

Il diritto penale o meglio la giustizia penale, come quella civile e amministrativa, ha quindi bisogno dell'IA che sia però governata in modo da prevenire errori predittivi o per individuare piste indiziarie sterili [32]. Il rischio è insito nella progressiva autonomia di elaborazione di

———

[28] In una moderna prospettiva sanzionatoria per reati appartenenti a questa categoria, ci sia consentito ancora rinviare a P. Troncone, *La tutela penale della riservatezza e dei dati personali cit.*, p. 79.

[29] M. Gialuz, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, in *www.penalecontemporaneo.it*, 29 maggio 2019. C. Parodi - V. Sellaroli, *Sistema penale e intelligenza artificiale: molte speranze e qualche equivoco*, in *www.penalecontemporaneo.it*, 16 giugno 2019. R. Bichi, *Intelligenza digitale, giurmetria, giustizia predittiva e algoritmo decisorio. Machina sapiens e il controllo sulla giurisdizione*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica, Il diritto, i diritti, l'etica*, Giuffrè, 2020, p. 424.

[30] Segnala la problematica A.M. Maugeri, *L'uso di algoritmi predittivi per accertare la pericolosità sociale: una sfida tra evidence based practices e tutela dei diritti fondamentali*, in *www.archiviopenale.it*, 17 maggio 2021.

[31] G. Ubertis, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, *www.sistemapenale.it*, 11 novembre 2020, p. 10.

[32] S. Quattrocolo, *Equità del processo penale e automated evidence alla luce della Convenzione europea dei diritti dell'uomo*, in *Revista Italo-Española de Derecho Procesal*, 2019, p. 2. L. Luparia - G. Ziaccardi, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Giuffrè, 2007.

circostanze e dati della realtà che la macchina per pensare acquisisce cercando di affrancarsi dall'uomo (33).

È naturale che conti essenzialmente l'immissione corretta dei dati e la corretta indicazione delle piste informatiche da elaborare, così come conta il controllo sugli esiti di congruità e di attendibilità cui giunge l'attività di elaborazione (34). Occorre, quindi, apprestare risorse che toccano più ambiti disciplinari per impostare correttamente l'uso dell'IA, con la presenza non solo di operatori del settore giudiziario, ma anche di criminologi, sociologi, assistenti sociali, tutte quelle risorse, insomma, che possano elaborare un modello integrato sempre più definito e attendibile (35).

Il ricorso alla c.d. *giustizia robotica*, ossia le decisioni giudiziarie assunte attraverso l'elaborazione del caso con il richiamo ai precedenti giudiziari (36) che possano con quello in esame trovare esatta riconduzione per applicare la medesima decisione, suscita perplessità soprattutto se si inquadra nella giustizia penale (37).

Questo nuovo futuribile assetto decisorio sarà chiamato a fare i conti anche con il principio di imparzialità del giudice che in questo caso potrebbe leggersi come errore della decisione (38).

Va considerato, inoltre, che i principi di tassatività e legalità sostanziale potrebbero subire una seria lesione per lo scarto logico che esiste tra valutazione e certificazione, laddove la prima rientra nella capacità del giudice umano di sussumere il caso sotto la previsione normativa corrispondente (39) e accertarne tutti gli aspetti soppesando i profili certamente rilevanti per la soluzione da adottare; l'attività di certificazione o constatazione svolta dall'operatore tecnico invece è una semplice presa d'atto di un precedente, di una vicenda già nota la cui conseguenza va ribadita (40).

Il vero problema è quello della prova, della ricerca dei frammenti probatori e la necessità di una lettura critica del materiale indiziante raccolto cha va ragionevolmente selezionato e coordinato, fino a subire il vaglio dibattimentale di confronto con elementi probatori di segno contrario (41).

La decisione ragionata e attendibile nasce da una valutazione intrinseca di questa com-

———

(33) C. Burchard, *L'intelligenza artificiale come fine del diritto penale?*, in *Riv.it. dir. e proc. pen.*, 2019.

(34) G. Riccio, *Ragionando su intelligenza artificiale e processo penale*, in *www.archiviopenale.it*, 21 novembre 2019.

(35) Va segnalata l'esperienza di giustizia predittiva nella materia civile nata dalla collaborazione del Tribunale e della Corte di Appello di Brescia con i Dipartimenti di Giurisprudenza e Ingegneria dell'Università di Brescia, in *www.giustiziapredittiva.unibs.it*.

(36) O. Di Giovine, *Il judge.bot e le sequenze giuridiche in materia penale (intelligenza artificiale e stabilizzazione giurisprudenziale)*, in *questa rivista*, 2020, p. 965. Interessante e tipica di quel Paese l'esperienza della Cina, in cui le giurisdizioni inferiori hanno formato raccolte di precedenti cui riferire la decisione automatiche per casi simili, in V. Capasso, *L'intelligenza artificiale come vettore di legal transplaint: la suprema Corte del popolo dal "caso" al "precedente"*, in *Riv. trim. dir. e proc. civ.*, p. 157.

(37) G. Canzio, *Il dubbio e la legge*, in *www.penalecontemporaneo.it*, 20 luglio 2018. M. Luciani, *La decisione giudiziaria robotica*, in *www.rivistaaic.it*, 30 settembre 2018. A. Traversi, *Intelligenza artificiale applicata alla giustizia: ci sarà un giudice robot*?, in *www.questionegiustizia.it*, 10 aprile 2019.

(38) F. Romeo, *Algoritmi di giustizia ed equità nel diritto. Quando razionalità ed emozionalità convergono*, in *www.i-lex.it*.

(39) N. Irti, *La crisi della fattispecie*, in *Riv. dir. proc.*, 2014, p. 37.

(40) G. Canzio, *Nomofilachia e diritto giurisprudenziale*, in Aa.Vv., *Il vincolo giudiziale del passato. I precedenti*, di A. Carleo (a cura), Il Mulino, 2018, p. 31.

(41) S. Quattrocolo, *Processo penale e rivoluzione digitale: da ossimoro a endiadi?*, in *MediaLaws*, 20 novembre 2019.

plessa raccolta indiziaria che difficilmente una struttura algoritmica sarà in grado di garantire (42).

5.2. La responsabilità penale per l'uso dell'IA: dall'uomo alla macchina e ritorno dalla macchina all'uomo

Il nuovo tema sul tappeto, dopo quello che ha già visto all'attenzione degli esperti la tutela civile contro l'uso dell'IA, è quello che investe la possibile tutela penale contro fatti che vedano l'IA come mezzo di consumazione di reati.

Venendo, dunque, al quesito se l'IA ha bisogno del diritto penale, si tratta in buona sostanza di ampliare l'oggetto materiale della tutela nell'ambito di provvedimenti legislativi già in essere, per un verso, e di assicurare iniziative di incriminazioni per fatti strettamente connessi ai rischi che comporta il ricorso a sistemi di IA.

Si è detto della necessità di ricercare le coordinate di un bene giuridico di nuovo conio inserito in una preesistente area di tutela penale da ampliare, con l'intera grammatica del diritto penale impegnata verso un interesse del tutto nuovo destinato ad aumentare la sua influenza nel rapporto: libertà dell'uomo-indipendenza della macchina (43).

A queste condizioni occorre rispondere positivamente al quesito posto, nel senso che, per i comportamenti estremi che costituiscono violazione di obblighi e divieti posti a protezione di valori in gioco così importanti, la risposta non può che essere affidata al diritto penale.

Peraltro, accanto alla più ampia dimensione teleologica si pone il problema dell'ampliamento della base dei soggetti punibili, come incremento della categoria dell'autore su cui grava la responsabilità e, dunque, la realizzazione del rischio (44).

L'individuazione del soggetto responsabile dell'elaborazione dei dati nel sistema dell'IA è in realtà il momento più vulnerabile del nuovo quadro normativo, poiché il trattamento potrebbe non essere completamente controllabile da parte dell'operatore fisico, così come potrebbe non esserci la evidenza di una causazione materiale del fatto che dà luogo all'evento (45). Potrebbe diventare arduo stabilire chi abbia attivato quella causa tra i vari contributi causativi che hanno dato vita all'elaborazione del trattamento di IA avvenuto poi in piena autonomia dalla macchina intelligente, dal meccanismo robotico (46).

Su questo terreno occorre mantenere nettamente distinti gli ambiti della responsabilità da prodotto e responsabilità da servizi, sebbene siano già oggetto di specifiche, seppur parziali, norme regolative. Così come vanno tenute nettamente distinte le responsabilità degli autori degli illeciti che si differenziano in proprietari, operatori e fornitori di servizi (cui non sono estranee le ipotesi di delega della funzione), le cui qualifiche soggettive designano anche il momento e la portata del loro intervento.

———

(42) S. Quattrocolo, *Quesiti nuovi e soluzioni antiche? Consolidati paradigmi normativi vs rischi e paure della giustizia digitale "predittiva"*, in *questa rivista*, 2019, p. 1764.

(43) S. Riondato, *Robot: talune implicazioni di diritto penale*, in P. Moro, C. Sarra (a cura di), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica, Franco Angeli*, Milano, 2017, p. 85. R. Borsari, *Intelligenza Artificiale e responsabilità penale: prime considerazioni*, in *MediaLaws*, 24 dicembre 2020.

(44) M. Bassini - L. Liguori - O. Pollicino, *Sistemi di Intelligenza Artificiale, responsabilità e* accountability. *Verso nuovi paradigmi?*, in F. Pizzetti (a cura di), *Intelligenza artificiale cit.*, p. 334.

(45) Problematiche messe opportunamente in luce da Magro M.B., *Robot, cyborg e intelligenze artificiali*, in *Cybercrime*, diretto da A. Cadoppi - S. Canestrari - A. Manna - M. Papa, Utet, 2019, p. 1179.

(46) A. Cappellini, *Machina delinquere non potest? brevi appunti su intelligenza artificiale e Responsabilità penale*, in *Criminalia*, 2018, p. 499.

Per quanto concerne il prodotto, vale a dire il sistema di IA messo in commercio e utilizzato secondo le istruzioni impartite dal produttore, soccorre la Direttiva europea 85/374/CEE che stabilisce le condizioni e le ipotesi punitive nel caso di accertato danno da prodotti difettosi. Il tema è ampiamente noto alla materia penale e tocca gli ambiti più sensibili della dogmatica, coinvolgendo il modello causale adottato dal nostro codice e il principio costituzionale di personalità della responsabilità penale (47).

Più significativo, per molti versi assolutamente nuovo, è il tema della responsabilità per l'uso dell'IA in presenza di un prodotto integro chiamato a svolgere applicazioni e sviluppo di IA per il settore dei servizi. A questo punto occorre effettivamente riflettere sulle conseguenze che l'attività della macchina intelligente ad apprendimento progressivo e autonomo può generare se l'operatore umano ne attiva il funzionamento e, indipendentemente dai suoi successivi interventi correttivi, lascia che il sistema di IA compia sempre nuove e diverse operazioni.

Il percorso uomo-macchina, tendendo conto dei livelli di rischio standardizzati, potrebbe condurre l'autonomia del sistema a compiere attività vietate ricadenti nel settore del rischio inaccettabile e vietato.

Il vero dilemma consiste nel fatto che la nuova e imprevista situazione attiva un nuovo percorso fatto da uomo-macchina-uomo, la cui responsabilità va ricercata in capo all'operatore che risponde per fatto illecito commesso da un sistema operativo fondato sulla autogestione evolutiva delle operazioni.

Sul piano civilistico l'accertata responsabilità patrimoniale può essere fondata sull'attribuzione colpevole del danno, ma anche sulla responsabilità oggettiva ricadente comunque sull'operatore (48).

Una soluzione potrebbe essere di assimilare i danni prodotti dalla macchina pensante alla responsabilità civile per la proprietà o il possesso di un veicolo a motore, per cui la legge impone la polizza assicurativa obbligatoria.

Si potrebbe immaginare la costituzione di un fondo di garanzia patrimoniale per fronteggiare il rischio di difficile monetizzazione, imponderabile negli effetti allo stato delle nostre conoscenze, proprio nella prospettiva del fine di non discriminazione (49).

Cosa del tutto diversa investe la materia penale in cui le ipotesi di responsabilità punibile devono essere fondate su condotte personali e colpevoli, secondo lo statuto di garanzia di libertà della persona delineato dalla nostra Carta fondamentale con l'art. 27. I presidi di garanzia devono essere individuati in tutte le attività che precedono l'uso del sistema di IA, ipotizzando una responsabilità che possa essere rimproverata per non aver seguito le prescrizioni e non aver previsto ciò che era ragionevolmente prevedibile alla luce della conoscenza tecniche dell'operatore aggiornato.

Esclusa la responsabilità oggettiva, l'estremo limite di rimprovero potrebbe essere limitato soltanto alle condotte poste in essere con colpa cosciente o dolo eventuale, ma anche in questi casi di tratta di entrare in un campo dove il nodo del principio di responsabilità personale

———

(47) C. Piergallini, *Danno da prodotto e responsabilità penale. Profili dommatici e politico-criminali*, Giuffrè, 2004.

(48) P. Serrao d'Aquino, *La responsabilità civile per l'uso di sistemi di intelligenza artificiale nella Risoluzione del Parlamento europeo 20 ottobre 2020: "Raccomandazioni alla Commissione sul regime di responsabilità civile e intelligenza artificiale"*, in *www.giustiziainsieme.it*, 18 novembre 2021.

(49) Come suggerisce G. Finocchiaro, *Intelligenza Artificiale*, cit., p. 1676.

colpevole registra le più alte tensioni in materia penale con i principi di garanzia della persona [50].

Diverso è il discorso che può tenere conto di una posizione di garanzia che l'operatore assume rispetto all'ordinamento e che per la materia penale, oltre che fondato sul nesso causale, si possa muovere anche un rimprovero per aver agito nella consapevolezza dell'evento tipico realizzato.

L'attribuzione del fatto illecito potrebbe trovare la sua plausibile fondatezza nella disciplina del II comma dell'art. 40, non avendo impedito l'evento in presenza di un obbligo giuridico specifico eluso, fino a considerare la disciplina generale che traccia il modello causale nell'ordinamento penalistico italiano regolato dall'art. 41 c.p., per effetto delle cause addizionali e concorrenti attivate dalle possibili molteplici condotte poste in essere da soggetti diversi nel corso dell'elaborazione, in cui si intrecciano condotte umane e condotte robotiche [51].

Tutto questo però ha un senso se alla base esiste un sistema di prescrizioni precise e aggiornate che stabiliscano la pista d'azione che deve condurre l'operatore a compiere le operazioni di intelligenza artificiale per le quali il sistema è stato progettato e rodato. Se ad esempio un operatore pubblico ritenesse di acquisire immagini senza l'autorizzazione del giudice, trattandosi di un intervento connotato da alto rischio e addirittura vietato da espresse prescrizioni limitative, nel violare quanto sancito commetterebbe un illecito penale se il legislatore provvederà in tal senso nei prossimi tempi.

Una diversa questione, invece si presenta quando si prospetta la possibilità che l'IA riuscirà ad affrancarsi progressivamente dalla persona umana che la controlla e ad assumere una gestione operativa sempre più autonoma e indipendente, diventerà difficile stabilire a priori a quale persona fisica personalmente responsabile sia da ascrivere la condotta (l'operazione di trattamento) vietata.

Il tema mostra serie varianti di rilevanza quando si tiene presente che il trattamento da IA può coinvolgere interessi di singoli più o meno importanti e, quindi, agire con diversa intensità del dolo, con più o meno consapevolezza e colpevolezza, con condotte attive oppure omettendo attività di controllo da posizioni di garanzia (e quali?) che sarebbero bastate a impedire l'evento [52].

Scattano a questo punto i presidi di garanzia stabiliti dalla stessa bozza di Regolamento sul versante dei rischi preventivati e la responsabilità si fonda non sulla maldestra operazione compiuta, ma sul fatto che l'operatore non ha preventivamente controllato che la macchina di IA, nella sua autonoma evoluzione tecnologica, basata sulla innovativa capacità di avanzamento, non ha inibito quelle operazioni che non rientravano più nel protocollo preventivamente stabilito per l'uso di quella macchina.

Ecco che allora soccorre un altro profilo introdotto dalla bozza di Regolamento, quello di aggiornare i casi e i livelli di rischio, in ragione dell'avanzamento imprevedibile che nasce dall'autonoma maturazione tecnologica del sistema di IA.

Solo a queste condizioni potrà essere mosso un rimprovero per la responsabilità penale dell'uomo, come mero ritorno di una vicenda operativa che sembrava affidata esclusivamente

———

[50] P. Severino, *Intelligenza artificiale e diritto. Parte I Le implicazioni dell'intelligenza artificiale nel campo del diritto con particolare riferimento al diritto penale*, in Aa.Vv., *Intelligenza artificiale*, cit., p. 104.

[51] M. Ienca, *Intelligenza2. Per un'unione di intelligenza naturale e artificiale*, Rosenberg & Sellier, 2019.

[52] D. Falcinelli, *Il dolo alla ricerca di una direzione penale. Il contributo della scienza robotica ad una teoria delle decisioni umane*, in *www.archiviopenale.it*, 14 marzo 2018.

alla macchina e che invece ha visto l'elusione del controllo preventivo da parte dell'operatore dedicato.

Le tre qualifiche soggettive del soggetto agente sposta anche più avanti il confine della responsabilità, fini a ricomprendervi la responsabilità amministrativa delle persone giuridiche del d.lg. n. 231/2001, trattandosi di soggetti, il proprietario, l'operatore, il fornitore di servizi o loro delegati, dipendenti di una persona giuridica privata tale da far scattare la responsabilità amministrativa dell'Ente di appartenenza. Anche questo potrebbe essere un valido presidio di responsabilità per assicurare ai terzi danneggiati una quota risarcitoria per il danno subito quando il reato è commesso nell'interesse o a vantaggio dell'Ente.

La notevole incertezza che la materia presenta al giurista contemporaneo impone, dunque, di valutare gli effetti del danno e del rischio, tentando di individuare le forme di indennizzo più adeguato che vadano ben al di là della risarcibilità patrimoniale da parte del solo soggetto responsabile [53].

La vittima di questi reati potrebbe rimanere del tutto scoperta dalla tutela risarcitoria per l'impossibilità di risalire all'effettivo autore, salvo ipotizzare forme di responsabilità oggettiva o per fatto altrui nel contesto normativo civilistico, ma del tutto estraneo all'ambito della materia penale, per cui sarà sempre l'uomo a risponderne nella cornice dei limiti possibili, essendo arduo ipotizzare una responsabilità robotica.

———

[53] F. Sgubbi, *Il reato come rischio sociale. Ricerche sulle scelte di allocazione dell'illegalità penale*, Il Mulino, 1990.

www.giuffre.it/riviste/penale